CONSIDÉRATIONS LIÉES À LA SÉCURITÉ DANS LE CADRE DE L'UTILISATION DE LOGICIELS LIBRES

Juillet 2020

ITSAP.10.059

Une organisation qui souhaite acquérir de nouveaux logiciels peut envisager d'utiliser les produits libres tout autant que les produits commerciaux. Les logiciels libres comportent certains avantages, car leur code source est accessible au public, ce qui en font une option abordable et souple pour les organisations. Or, ils peuvent engendrer leur lot de surprises. Bien qu'ils soient pratiques, les logiciels libres peuvent comporter des vulnérabilités et des risques pour la sécurité de votre organisation. Le présent document fait état de ces risques ainsi que des mesures à prendre pour les atténuer.

CODE SOURCE OUVERT

Le code source ouvert est créé grâce à la collaboration de spécialistes en développement de logiciels. Les auteurs du code mettent les logiciels sous un type de licence qui permet à quiconque de voir, de modifier et de distribuer le code en question, voire d'en créer de nouvelles versions. Dans ce cas, les développeurs peuvent élaborer davantage le code dans le but de créer un produit logiciel autonome ou d'ajouter de nouvelles fonctionnalités à celles qui existent déjà.

Les logiciels libres sont couramment utilisés. Il est probable que vous connaissiez déjà un certain nombre de produits dont le code source est ouvert, notamment les navigateurs Google Chrome et Firefox. Comme l'accès à ces produits est libre, n'importe qui peut apporter des modifications au code existant. Cette accessibilité intégrale facilite l'adaptation des produits libres aux besoins de l'entreprise. Ainsi, des fonctionnalités peuvent être ajoutées, supprimées ou modifiées à loisir.

78 % des entreprises utilisent des logiciels libres, mais moins de la moitié d'entre elles les gèrent de façon appropriée

- Résultats d'un sondage mené en 2016 sur l'avenir de code source libre

RISQUES

Avant d'utiliser des logiciels libres au sein de votre organisation, vous devriez tenir compte des risques qu'ils comportent. En voici quelques exemples :

- **Accès déraisonnable** – Le code source ouvert est accessible à tous, ce qui permet aux auteurs de cybermenace de manipuler le code à des fins malveillantes. Lorsque votre organisation emploie des logiciels qui ont été modifiés de la sorte, elle expose son réseau et ses informations aux accès non autorisés.
- **Lacunes en matière d'assurance de la qualité** – Il n'est pas toujours certain que des experts ont mené des tests rigoureux visant à garantir la qualité du produit pendant toutes les phases de développement du logiciel libre ni que ceux qui ont examiné le code ont minutieusement vérifié toutes les fonctions de sécurité. Ces lacunes posent des risques pour l'infrastructure de TI de votre organisation.
- **Manque de soutien technique** – La majorité des logiciels libres n'offrent pas de services de soutien. Sans une équipe de soutien, les mises à jour et les correctifs essentiels ne sont pas forcément disponibles. Par conséquent, lorsque des vulnérabilités sont détectées, les auteurs malveillants ont tout le loisir de les exploiter pour tenter d'accéder au réseau, aux systèmes et à l'information de votre organisation. Il revient au groupe qui se charge de la maintenance du logiciel libre de signaler toute vulnérabilité connue et de développer les correctifs nécessaires.

Les produits libres n'affichent pas tous le même niveau de risque. De fait, certaines composantes de plusieurs produits commerciaux contiennent du code source ouvert. Prenons par exemple les fournisseurs de produits de sécurité des TI qui comportent des fonctionnalités cryptographiques. Ces fournisseurs intègrent la bibliothèque cryptographique OpenSSL libre dans leurs produits.

Avant de vous procurer et de mettre en place des logiciels libres, il est essentiel de mener des activités d'assurance de l'information. Ces activités vous permettront de continuer à protéger les réseaux, les systèmes et l'information de votre organisation.

CYCLE DE VIE DU DÉVELOPPEMENT DE LOGICIELS LIBRES

Les termes « logiciel libre » et « code source ouvert » font référence à une approche de développement de programmes informatiques qui repose sur les valeurs de la collaboration, de la transparence et du développement axé sur la communauté. Le cycle de vie du développement de logiciels libres comporte plusieurs étapes, notamment l'analyse des besoins, la conception, la mise en œuvre, les tests, la livraison et la maintenance. Dans certains cas, de grandes entreprises soutiennent des projets de développement de logiciels libres, mais ceux-ci dépendent peut-être d'activités menées dans le cadre de petits projets de logiciels libres gérés par des bénévoles.

L'équipe de projet rend publics les logiciels libres dès qu'elle les a mis en marche, même s'ils contiennent des bogues. L'inspection et l'examen de ces logiciels par le public sont souvent nécessaires pour améliorer le produit au fil du temps. Des volontaires testent le logiciel et formulent des commentaires pour signaler les bogues et suggérer des mesures correctives. En tenant compte de ces commentaires, les membres de l'équipe de projet du logiciel préparent la prochaine version du logiciel. Ces étapes sont répétées autant de fois qu'il le faut pour améliorer le logiciel et lancer des versions stables.

Dans le cas des petits projets de logiciels libres, les bénévoles auront peut-être moins de temps à consacrer à la résolution de problèmes ou à la réalisation des tests de sécurité. Certains projets ne disposent pas des fonds nécessaires pour embaucher des vérificateurs spécialisés en sécurité. De plus, la sécurité n'est pas nécessairement intégrée à la conception et au développement de logiciels libres, ce qui peut donner lieu à des vulnérabilités et comporter des risques pour votre organisation.

PROTÉGEZ VOTRE ORGANISATION

Veillez à ce que votre organisation se soit dotée d'un cadre de sécurité des TI. Ce cadre doit comporter les éléments suivants :

- **Politique organisationnelle pour la sécurité des TI** – Une politique claire et rigoureuse en matière de sécurité des TI fait état des méthodes de travail et de collaboration que les employés doivent suivre relativement à l'utilisation des réseaux, et énonce la position de l'organisation à l'égard de la gestion des risques de sécurité. Il convient également d'examiner le cadre et, s'il y a lieu, de le mettre à jour assez fréquemment pour qu'il réponde à l'environnement de menaces actuel.
- **Attribution des ressources** – Il faut également définir les rôles et les responsabilités qui incombent aux administrateurs de système, en plus de limiter le nombre des intervenants qui jouiront de ce type d'accès privilégié.
- **Procédures d'administration des systèmes** – En dernier lieu, il faut convenir de procédures qui définissent la façon dont les administrateurs de systèmes seront appelés à gérer et à entretenir, en toute sécurité, les réseaux et les logiciels de l'organisation.

POINTS À CONSIDÉRER AVANT D'UTILISER DES LOGICIELS LIBRES

En fin de compte, l'utilisation de logiciels libres devrait cadrer avec la stratégie globale de TI de votre organisation, mais voici quelques facteurs à prendre en considération si vous choisissez d'utiliser des logiciels libres.

Avant d'acheter un nouveau logiciel : Votre organisation devrait établir le niveau de risque qu'elle est disposée à tolérer et à accepter. Par la suite, vous serez en mesure de déterminer quels produits logiciels vous pouvez vous permettre d'utiliser et choisir ceux qui répondent à vos besoins opérationnels et à vos exigences en matière de sécurité.

Avant d'installer un nouveau logiciel : Votre organisation devra prendre les mesures nécessaires pour détecter et atténuer les vulnérabilités (journaux, audits, processus d'intervention en cas d'incident, etc.). Faites toujours la mise à l'essai d'un logiciel avant de l'installer, et effectuez ces tests tout au long du cycle de vie du logiciel, notamment avant l'installation de mises à jour et de correctifs. La surveillance continue et les tests permettent de réduire les risques d'exploitation.

Pendant l'utilisation des logiciels libres : Vous devriez gérer tous les logiciels libres au moyen des procédures et outils que vous employez pour les produits commerciaux. Comme toujours, il convient de veiller à ce vos employés suivent de la formation sur les pratiques exemplaires en cybersécurité pour les aider à utiliser et à gérer les produits logiciels en toute sécurité.

Vous avez des questions ou vous avez besoin d'aide? Vous voulez en savoir plus sur les questions de cybersécurité? Consultez le site Web du Centre canadien pour la cybersécurité (Centre pour la cybersécurité) à **cyber.gc.ca**.