Produits obsolètes

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Mars 2023 | ITSAP.00.095

Les organisations comme la vôtre investissent de grosses sommes pour se procurer les biens de technologies de l'information (TI) nécessaires à leurs opérations. La plupart de ces biens (tant matériel que logiciel) ont une durée de vie limitée, car ils deviennent dépassés ou même obsolètes. En fait, même s'ils fonctionnent encore, ils peuvent mettre votre organisation à risque s'ils continuent d'être utilisés. La pratique exemplaire veut que les technologies obsolètes soient abandonnées. Toutefois, dans les faits, les organisations ont besoin de temps pour mettre à niveau ou remplacer les biens de TI. Le présent document contient des astuces pour minimiser les risques que votre organisation court au moment où elle abandonne progressivement ses produits obsolètes.

Qu'est-ce qu'un produit obsolète?

Selon la Commission électrotechnique internationale (CEI), un produit est obsolète lorsqu'il n'est plus produit par le manufacturier selon les spécifications originales [IEC 62402]. Les fournisseurs de produits prennent la décision stratégique d'éliminer progressivement un produit dans le but de le supprimer graduellement ou de le retirer. Ils peuvent aussi abandonner une gamme de produits qui coûte trop cher à exploiter ou à maintenir. Ainsi, ils arrêtent de prendre en charge (mises à jour de sécurité, corrections de bogues et mises à niveau) les versions les plus anciennes de leurs produits.

Quels sont les risques liés aux produits obsolètes?

Il n'est pas rare pour les organisations d'exploiter leurs biens de TI jusqu'à ce qu'ils soient dépassés ou bien au-delà du cycle de remplacement suggéré. Tant que les biens dépassés ou patrimoniaux sont pris en charge par le fournisseur, ils représentent un risque faible. Toutefois, si votre organisation utilise, pour une durée prolongée, des biens obsolètes sans avoir de plan pour les mettre à niveau ou les remplacer, elle court un risque élevé de compromission. Voici certains des risques:

Vulnérabilités informatiques. Les produits obsolètes qui ne reçoivent plus de mises à jour de sécurité sont plus vulnérables aux cyberattaques. Les problèmes ou les vulnérabilités mis au jour pour ces produits ne seront pas corrigés et peuvent devenir des vecteurs d'attaque que les auteures ou auteurs de menace peuvent exploiter.

Plantage et inaccessibilité du système. Les logiciels obsolètes finiront par ne plus fonctionner sur le nouveau matériel et par ne plus être compatibles avec les systèmes d'exploitation récents. Cela peut mener à de l'instabilité, à une performance défaillante ou au fonctionnement inadéquat du système et provoquer du plantage et des périodes d'indisponibilité. Pour l'organisation, cela peut représenter une interruption des activités et donc une perte de revenu.

Augmentation des coûts financiers. Il peut s'avérer très coûteux de conserver des produits ou des systèmes obsolètes au-delà de leur période d'élimination progressive. Le fournisseur de produit (ou un fournisseur tiers) peut exiger des primes pour continuer la prise en charge. Des ressources internes additionnelles peuvent aussi être nécessaires.

Conformité juridique et réglementaire. L'utilisation de produits obsolètes ou non pris en charge peut représenter un risque accru insoupçonné de non-conformité. Le fait de ne pas abandonner un logiciel non pris en charge ou des systèmes patrimoniaux expose l'organisation à des peines réglementaires, à des poursuites, à des engagements financiers ou à des suspensions d'activités.

Présence de produits obsolètes dans les systèmes de contrôle industriels (SCI) et les technologies opérationnelles (TO)

La fiabilité est un des éléments essentiels pris en compte lors de la conception et de la mise sur pied des SCI et des TO. Cela est primordial, car ils jouent tous deux un rôle de premier plan dans le soutien et la gestion des infrastructures essentielles. Le cycle de vie des SCI et des TO est beaucoup plus long que celui d'autres systèmes; plus les composants vieillissent, plus ils sont difficiles à réparer ou à remplacer. De plus, il est peu probable que les systèmes obsolètes soient pris en charge par les fabricants ou les fournisseurs. Pour cette raison, il incombe aux exploitants et aux propriétaires des SCI et des TO de prendre les devants et de prévoir le remplacement de ces systèmes et de leurs composants bien avant leur obsolescence. Si le remplacement n'est pas possible, il convient d'adopter des mesures d'atténuation pour protéger les systèmes. Pour être efficace, un plan d'atténuation de l'obsolescence doit comprendre les éléments suivants:

- des politiques sur la sauvegarde et les produits de rechange qui tiennent compte de l'indisponibilité de produits de remplacement en raison des conditions du marché;
- des programmes pour veiller à ce que l'organisation dispose des ressources internes suffisantes pour remettre sur pied des systèmes ayant une configuration réputée bonne et que ces ressources soient formées adéquatement;
- des pratiques exemplaires concernant la protection des produits nécessitant une connexion Internet, infonuagique ou sans fil;
- des processus de vérification approuvés pour choisir des fournisseurs qui offrent des services de planification du cycle de vie, notamment des estimations de moyenne des temps de bon fonctionnement (MTBF) ainsi que des préavis de dates de fin de prise en charge;
- des contrôles de sécurité à déployer avant la date de fin de prise en charge pour protéger les réseaux des SCI et des TO. Pour obtenir de plus amples informations, veuillez consulter Facteurs relatifs à la sécurité à considérer pour les systèmes de contrôle industriels (ITSAP.00.050) et Protéger vos technologies opérationnelles (ITSAP.00.051).

Centre de la sécurité des télécommunications
Communications Security Establishment

Canada

Produits obsolètes

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Mars 2023 | ITSAP.00.095

Comment gérer les risques que représentent les produits obsolètes

La première étape, qui est aussi la plus importante, pour gérer les risques que représentent les produits obsolètes consiste à faire l'**inventaire** des biens de TI (matériel et logiciel) de votre réseau. Répertorier soigneusement tous les biens en prenant soin de noter leur type et leur version. La prochaine étape est de **relever** les biens qui ne sont plus pris en charge par un fournisseur ou qui sont en fin de vie. Pour minimiser les risques d'éventuelles cyberattaques et réduire l'incidence d'une compromission, songez à adopter les **mesures d'atténuation à court terme** suivantes.

- ☐ **Déconnectez** du réseau **les appareils obsolètes** qui ne sont plus utilisés et qui ne sont pas nécessaires aux opérations.
- ☐ **Instaurez des zones de sécurité de réseau** pour contrôler les accès aux composants obsolètes et les flux de données depuis ces composants et vers ceux-ci. Segmentez les réseaux en plus petites portions. Ainsi, il sera plus difficile pour un rançongiciel d'infecter l'ensemble du réseau. Pour obtenir de plus amples informations, veuillez consulter Les 10 mesures de sécurité des TI visant à protéger les réseaux Internet et l'information (ITSM.10.089).
- ☐ **Recourez à des outils de sécurité préventive, comme des antimaliciels, des antivirus et des coupe-feu, ainsi qu'à un un système de détection des intrusions sur l'hôte (SDIH)** pour réduire les risques liés aux intrusions malveillantes (maliciel, logiciel espion, utilisatrices ou utilisateurs non autorisés, etc.). Comme les systèmes obsolètes ne sont probablement pas mis à jour, les outils de sécurité peuvent être moins efficaces.
- ☐ **Limitez les connexions des composants obsolètes aux réseaux non fiables, comme Internet**. Si cela n'est pas possible, bloquez l'accès au contenu Web et au média enrichis (macros et modules d'extension de navigateurs Web). Procédez à l'analyse des vulnérabilités à la périphérie de réseau pour détecter le trafic malveillant entrant. Cette mesure minimise le risque qu'un maliciel atteigne les composants obsolètes du système.
- ☐ **Empêchez l'accès à des dispositifs de stockage amovibles**, comme des clés USB, qui peuvent transmettre du contenu malveillant aux appareils obsolètes. Bloquez l'accès à de tels dispositifs en désactivant les ports USB ou en interdisant l'accès par la stratégie de groupe.
- ☐ **Vérifiez les services qui fonctionnent sur les serveurs obsolètes** et déconnectez ou désactivez ceux qui ne sont pas essentiels. Les services requis devraient être déplacés vers des serveurs pris en charge ou des services infonuagiques.
- ☐ **Procédez à la journalisation, à la surveillance et à la vérification** des composants obsolètes du système. Cette action va permettre la détection des types d'attaques lancées contre les composants et la mise en œuvre subséquente de mesures d'atténuation proactives. Pour de plus amples renseignements, veuillez consulter les documents Journalisation et surveillance de la sécurité de réseau (ITSAP.80.085) et Vérification de la sécurité des réseaux (ITSAP.80.086).
- ☐ **Élaborez un plan d'intervention en cas d'incident** qui comprend les processus, les procédures et les documents liés aux mesures de détection, d'intervention et de reprise que doit prendre l'organisation en cas de cyberattaque.
- ☐ **Supprimez et nettoyez les données des dispositifs ou des supports de stockage mis hors service** pour qu'elles ne soient pas récupérables ou consultables. Assurez-vous de faire une sauvegarde de données avant de nettoyer le dispositif.
- ☐ **Éliminez le matériel et les logiciels à la fin de leur cycle de vie.** Dans certains cas, la destruction physique d'appareils ou de supports (en plus du nettoyage approprié) est la meilleure façon de veiller à ce que les données sensibles ne soient pas accessibles. Pour obtenir de plus amples informations, veuillez consulter le document Nettoyage et élimination d'appareils électroniques (ITSAP.40.006).
- ☐ **Nettoyez régulièrement les produits obsolètes qui sont en utilisation** pour supprimer tout maliciel qui pourrait y être implanté. Il s'agit d'une mesure temporaire, car le dispositif restera vulnérable si le moyen d'attaque n'est pas bloqué.

La gestion de l'obsolescence à long terme

Voici quelques stratégies à long terme pour aider votre organisation à gérer efficacement les risques que représentent les produits obsoletes.

- Adoptez un programme de gestion des biens de TI pour suivre, surveiller et maintenir les biens de TI tout au long du cycle de vie, de l'approvisionnement jusqu'à l'élimination. Tirez le maximum des outils de gestion des biens de TI pour gérer efficacement les biens.
- Élaborez un plan de transition pour tous les biens de TI, du moment de leur approvisionnement jusqu'à la fin de la période de prise en charge. Le plan devrait comprendre le processus pour la mise à jour, la mise à niveau ou le remplacement du produit ainsi que la formation offerte au personnel sur l'utilisation des nouveaux systèmes.
- Songez à opter pour la prise en charge à vie du produit lors de l'achat de nouveau matériel ou de la licence d'un nouveau logiciel.
- Dans la mesure du possible, choisissez des produits offrant des formats de données ouvertes. Cette solution peut minimiser les problèmes possibles d'accès aux données verrouillées ou exclusives ou de migration de ces données.

Centre de la sécurité des télécommunications
Communications Security Establishment

Canada