AVEZ-VOUS OUBLIÉ LES FONDAMENTAUX ?

Voici une série de questions adressées notamment aux RSSI et aux DSI, issues du discours de Patrick Pailloux en clôture des Assises de la Sécurité des Systèmes d'Information 2011.

Combien de personnes disposent du mot de passe administrateur permettant d'accéder au système central de gestion des droits ?
Il convient de réduire le nombre de titulaires de comptes disposant de privilèges élevés aux seules personnes pour lesquelles ces privilèges sont nécessaires à l'accomplissement de leur mission. Des listes doivent être tenues à jour pour tous les comptes de ce type, dont évidemment les comptes permettant d'accéder au système central de gestion des droits, qui constituent des cibles de choix pour les attaquants.

Quel mot de passe est utilisé pour installer une imprimante ? Le mot de passe permettant le contrôle total de votre système d'information, ou un autre ?
Le partage de mot de passe entre comptes doit être banni.

Chaque administrateur dispose-t-il d'un mot de passe différent ?
Afin de limiter les risques de compromission du mot de passe et de favoriser la traçabilité des actions, chaque individu doit utiliser un mot de passe personnel.

Lorsqu'un administrateur travaille à autre chose qu'à des tâches d'administration, quel type de compte utilise-t-il ?
Les comptes avec des droits d'administrateur doivent être strictement réservés à l'exécution de tâche d'administration. Des procédures doivent avoir été définies et une charte de l'administrateur établie, afin de préciser ces conditions. Les administrateurs doivent utiliser un compte non privilégié lorsqu'ils effectuent des actions plus exposées, comme lire leurs courriels ou naviguer sur le Web.

Quand, pour la dernière fois, quelqu'un a-t-il vérifié qui disposait des droits d'accès à la messagerie de votre PDG ou DG ?
Les accès à des ressources sensibles, comme la messagerie de dirigeants, doivent faire l'objet d'une surveillance régulière.

Qui a vérifié si cette nuit, un fichier zip de 2 Go n'avait pas été extrait de votre système d'information ? Quelqu'un regarde-t-il de temps en temps si les flux sortant de votre SI, la nuit par exemple, sont légitimes ? Si les adresses de destination sont normales ? La dernière fois que vous êtes venus travailler un dimanche, quelqu'un est-il venu vous demander le lundi s'il était normal que quelqu'un se soit connecté sur votre compte dimanche ?
L'analyse des journaux d'évènements permet de repérer les activités inhabituelles et de détecter d'éventuels signes d'intrusion. Les journaux d'événements doivent être activés, configurés et centralisés pour permettre cette analyse. De plus, le système utilisé doit permettre de générer faciliter la génération d'alertes simples et l'organisation doit prévoir le personnel et les procédures permettant de traiter ces alertes.

Votre propre poste de travail est-il à jour de ses correctifs de sécurité (pour l'ensemble des logiciels installés) ?
Il convient de mener un inventaire logiciel pour tous les postes de travail et d'utiliser un système centralisé de gestion des mises à jour pour corriger les vulnérabilités des logiciels inventoriés. Il ne suffit pas de mettre à jour uniquement le système d'exploitation, mais bien l'ensemble de logiciels déployés sur son parc.

Votre SI comporte-t-il encore des applications tournant sur Windows XP pack 2, voire 2000, voire NT4 (on en voit plus souvent qu'on ne le penserait) ? Dans ce cas, quelles mesures de précaution ont été prises ?
Lorsqu'il n'est pas possible de migrer ces applications vers des systèmes maintenus par l'éditeur, il convient d'isoler de manière particulièrement restrictive et de porter une attention particulière à leurs journaux d'événements.

Quelqu'un a-t-il la cartographie de votre réseau — vraiment, pas juste une idée plus ou moins précise dans sa tête, mais un vrai schéma ?
Le maintien d'une cartographie à jour est indispensable pour pouvoir identifier les vulnérabilités et les corriger.
Elle permet également de pouvoir réagir rapidement en cas de détection d'intrusion en limitant les risques de créer des dysfonctionnements par méconnaissance de son système d'information.

Combien d'accès internet avez-vous ? Où sont-ils ? Sont-ils tous administrés ? Surveillés ?
De trop nombreuses organisations laissent se multiplier les accès internet « sauvages », comme des lignes ADSL. Le résultat est une perte de capacité de surveillance des flux entrants et sortants et de blocage des flux illégitimes. Les accès sauvages échappent

en effet aux systèmes de filtrage et de détection d'intrusion. Lorsqu'ils les identifient, des attaquants peuvent privilégier ces accès pour exfiltrer des données. Tout accès Internet doit donc être recensé dans la cartographie et des règles de filtrage et de surveillance adaptés doivent y être associées. Le nombre d'accès doit être le moins élevé possible.

Combien de temps se passe-t-il entre le moment où quelqu'un quitte votre organisation et le moment où son compte est supprimé ?
Tout compte devenu inutile doit être immédiatement supprimé. Dans le cas contraire, un attaquant peut l'utiliser discrètement — qu'il s'agisse de l'ancien titulaire du compte ou d'un attaquant externe tirant profit de la situation. Une procédure adaptée doit donc être mise en place pour que le service informatique soit informé en cas de départ d'un employé et puisse supprimer ses droits d'accès. Lorsqu'une personne dispose d'un compte temporaire dans l'organisme (ex : stagiaire, prestataire), une date d'expiration devrait être configurée dès la création du compte.

Combien avez-vous de comptes non individuels, de comptes de service ? À quoi servent-ils ?
Trop souvent les comptes partagés entre plusieurs individus ou de services possèdent des mots de passe faibles (type mot de passe=nom de compte) et qui n'expirent jamais. Or ces comptes permettent généralement d'accéder à de multiples ressources et, pour les comptes de services, disposent souvent de privilèges élevés. Pour ces raisons, ils sont l'une des premières cibles des attaquants. Il convient donc de tenir une liste de ces comptes et d'en mener une revue périodique pour en restreindre le nombre.

L'exécution automatique des supports usb est-elle désactivée ?
Les logiciels malveillants se diffusent très facilement par l'intermédiaire des supports USB lorsque l'exécution automatique de ces derniers est activée. Pour faciliter la gestion de cette fonctionnalité, vous pouvez utiliser des mécanismes de stratégie de groupe (GPO sous Windows) afin de désactiver les fonctions d'autorun et d'autoplay.

Les utilisateurs peuvent-ils installer des applications ?
Les utilisateurs ne doivent pas disposer de privilèges d'administrateurs. Par ailleurs, les stratégies de restrictions d'exécution logicielle (SRP et AppLocker sous Windows) limitent l'exécution de logiciels malveillants et empêchent l'utilisateur de lancer un programme depuis un média amovible ou son profil utilisateur. Il faut être vigilant aux environnements tels que Java, Adobe Air ou Perl, qui permettent d'exécuter des logiciels sans être contraints par les stratégies de restriction d'exécution logicielle.

Quel plan avez-vous en cas d'intrusion majeure dans votre système ?
Une intrusion d'ampleur dans un système d'information est une crise. Chaque heure qui passe peut notamment signifier la fuite d'informations stratégiques, avec dans certains cas, leur publication à des fins de déstabilisation. Des risques de suspension de l'activité de l'organisation sont aussi à prévoir. Un plan de réponse spécifique doit donc exister. Le plan de réponse doit prévoir les mesures organisationnelles et techniques permettant de délimiter au plus vite l'ampleur de la compromission et de la circonscrire. Par exemple, les documents nécessaires à la gestion de la crise, comme la cartographie du système, la liste des personnels en mesure d'intervenir sur les systèmes, les coordonnées des administrations susceptibles de porter assistance, doivent être tenus à jour et connus des personnels qui devront piloter la gestion de ce type de crise.

Que se passe-t-il quand vous découvrez un poste de travail compromis par un virus ? Le changez-vous simplement ou vérifiez-vous si par hasard l'attaquant n'aurait pas rebondi ailleurs dans votre système ?
La recherche d'éventuelles autres traces d'intrusion sur votre système est indispensable après la découverte d'une compromission. Généralement, les attaquants ne se contentent pas en effet de la compromission d'un ordinateur : ils s'ouvrent de multiples portes d'entrée dans le système afin de pouvoir revenir si d'aventure leur porte principale était refermée.