Chapitre
22

Chapitre 22: Annexes

Les articles et brochures suivants sont reproduits à la fin du document d'information :

NOTE D'INFORMATION DU CERTA, 9/11/2006 : Risques associés aux clés USB

Ce document informe les entreprises sur les risques présentés par les nouvelles catégories de clés USB.

Boursier.com, 18/05/2007 : Alcatel-Lucent : un disque de données salariés de Lucent envolé

Cet article révèle une retentissante affaire de vol de données. Mobilegov propose une solution pour lutter contre de tels vols.

Le Monde Informatique, 05/12/2007 : Les services informatiques, premiers responsables des fuites de données

Selon une étude du cabinet Orthus, 30 % des fuites de données sensibles trouvent leurs origines dans le service informatique de l'entreprise. Et elles auraient toutes pu être évitées en appliquant le règlement intérieur des sociétés.

Mobilegov permet aux collaborateurs d'utiliser leurs outils favoris, mais sans risque pour l'entreprise.

Réseaux-Télécom.net, 24/09/2007 : L'humain reste le maillon faible de la sécurité du SI

Dans son rapport annuel « 2007 Global Security Survey », le cabinet Deloitte Touche Tomatsu montre que les employés et les clients restent le plus grand facteur de risque d'une institution financière.

Site web IP Vista, 28/11/2007 : Communiqué de Presse informant de l'arrivée de Mobilegov

Site web du South-East England Development Agency, 04/12/2007 : Mobilegov opens an office in the 'UK Silicon Valley'

French security software editor Mobilegov launches its UK presence this autumn in Reading at the heart of the Thames Valley following several months of market research and supported by the Thames Valley Economic Partnership (TVEP), South East England Development Agency (SEEDA) and UK Trade & Investment (UKTI) in Paris.

Réseaux-Télécom.net, 21/09/2007 : La cybercriminalité se professionnalise

Selon le dernier Rapport sur les menaces à la sécurité Internet publié par Symantec, la cybercriminalité devient une activité de plus en plus professionnelle et commerciale. Les pirates et autres organisations criminelles cherchent à tirer toujours plus de profit de leurs attaques en ligne.

Zebulon.fr, 30/07/2007 : Device Linker, la clé USB sécurisée

Les clés USB ont depuis bien longtemps pris une place prépondérante dans notre quotidien. Pourtant, en cas de perte ou de vol, nos précieuses données peuvent se retrouver entre de mauvaises mains. De plus, en ce qui concerne les entreprises ou les administrations publiques, ces clés introduisent une nouvelle menace de sécurité où des données confidentielles peuvent facilement être dérobées. Face à ce constat, la société Mobilegov propose une clé USB sécurisée utilisable uniquement sur des PC autorisés.

Site web de la FNAC, 17/12/2007 : Device Linker - single soft

Device Linker® vous protège contre le vol de vos données sauvegardées sur votre clé U3 en cas de perte ou de vol. Tant que votre clé USB U3 ne reconnaît pas la configuration sur laquelle elle est connectée, elle reste inutilisable et l'accès aux données qu'elle contient est impossible !

01net, 20/12/2007 : L' « ADN numérique » des périphériques sécurise leurs connexions

Mobilegov propose une solution de gestion de la sécurité des équipements amovibles, dont les smartphones et les clés USB.
Avec Device Authenticator Pro Edition, la jeune pousse française Mobilegov fournit une solution élégante à un problème qui prend de l'importance en entreprise : la gestion des périphériques amovibles. Ces équipements sont de plus en plus sophistiqués et donc difficiles à contrôler.

Brochures commerciales Device Authenticator et Device Linker

Ces brochures, comme tous les documents techniques, existent en français et en anglais.

S . G . D . N
Direction centrale
de la sécurité des
systèmes d'information

Paris, le 09 novembre 2006
N° CERTA-2006-INF-006-001

Affaire suivie par :

CERTA

NOTE D'INFORMATION DU CERTA

Objet : Risques associés aux clés USB

GESTION DU DOCUMENT

Tableau 1: Gestion du document

Référence	CERTA-2006-INF-006-001
Titre	Risques associés aux clés USB
Date de la première version	09 novembre 2006
Date de la dernière version	14 novembre 2006
Source(s)	
Pièce(s) jointe(s)	Aucune

Une gestion de version détaillée se trouve à la fin de ce document.

1 INTRODUCTION

Les périphériques USB (pour Universal Serial Bus) occupent actuellement une place prépondérante dans l'univers de l'appareillage informatique. Ils peuvent être de tout type, comme par exemple un support de données amovible (clé USB, lecteur de musique au format MP3, etc).

De par leur facilité d'installation, ces périphériques s'échangent très facilement d'une machine à une autre. Cependant, cette opération présente des risques. Nous montrons dans ce document que ces échanges peuvent aussi bien affecter le périphérique que l'ordinateur d'accueil.

Du fait de la simplicité et de la furtivité des attaques basées sur ces échanges, il est important de prendre des mesures préventives. Il n'est bien sûr pas question de remettre en cause l'utilité de l'USB, notamment les différents périphériques de stockage, mais certaines considérations doivent être prises avant leur utilisation, que ce soit pour l'utilisateur ou l'administrateur. Ce document offre donc quelques recommandations à cet égard.

2 PRÉSENTATION DE L'*UNIVERSAL SERIAL BUS*

2.1 USB 1.0 et 2.0

L'USB (pour Universal Serial Bus) est une interface de connexion définie dans les années 90 et destinée à remplacer les ports série et parallèle sur les ordinateurs. Elle est utilisée de nos jours pour brancher tout type de périphérique, que ce soient les imprimantes, les scanners, les modems, ou des appareils de stockage, comme les clés USB.

Sans rentrer dans les détails fournis par les documents de référence, il existe, à la date de rédaction de cet article, deux standards distincts, USB 1.1 et USB 2.0 :

- L'USB version 1.1 considère deux modes différents, dits lent (1,5 Mbits/s en théorie) et rapide (12 Mbits/s en théorie). Le premier mode, moins sensible aux perturbations électromagnétiques, convient aux petits transferts de données, comme ceux requis par les claviers ou les souris. Le second peut servir dans le cas d'imprimantes, de scanners, de disques durs externes, ou de lecteurs et graveurs CD/DVDs.
- L'USB version 2.0 ajoute un nouveau mode, permettant des échanges théoriques à 480 Mbits/s. La compatibilité entre périphériques USB 1.1 et 2.0 est assurée. Toutefois l'utilisation d'un périphérique USB 2.0 sur un port USB à bas débit limitera celui-ci à 12 Mbit/s maximum. De plus, le système d'exploitation est susceptible d'afficher un message expliquant que le débit est bridé.

Les termes sont parfois utilisés de manière abusive, et la dénomination commerciale USB 2.0 Full Speed fait en réalité référence à la version USB 1.1 en mode rapide, tandis que USB 2.0 High Speed correspond bien au standard 2.0.

L'architecture de type USB a pour caractéristique de fournir une alimentation électrique aux périphériques qu'elle relie, avec une tension maximale de 5V et un courant d'au plus 500mA. Il est enfin possible de connecter jusqu'à 127 appareils à un Bus USB[1] à un temps donné. L'USB se compose de plusieurs couches de protocoles, ou moyens de communication, qui ne seront pas abordées dans ce document.

L'USB, pour résumer, possède les propriétés suivantes :

- la topologie en arbre dont la racine est normalement une machine hôte (PC, Mac, etc.) ;
- les périphériques peuvent être branchés et débranchés sans arrêter l'ordinateur ;
- les périphériques sont alimentés par un bus ;
- il est possible de chaîner jusqu'à 127 périphériques sur un même bus USB (avec l'utilisation d'un *hub* par exemple);
- les périphériques inutilisés sont automatiquement mis en veille ;
- les périphériques sont identifiés et configurés automatiquement par les systèmes d'exploitation.

2.2 La norme *On-the-Go*

L'USB est contrôlé par un hôte, installé sur la machine d'accueil. L'hôte USB a la charge de mener à bien toutes les transactions et de gérer la bande passante.

Cependant, depuis l'USB 2.0, il existe un protocole « au pied levé » (ou *On-the-Go*), qui permet, pour deux périphériques USB, de négocier et d'élire un hôte parmi eux. L'intérêt est le suivant : on peut relier deux périphériques sans ordinateur. Parmi les illustrations les plus courantes, il peut s'agir d'une imprimante et d'un appareil photo numérique reliés entre eux, ou bien d'un lecteur MP3 et d'une clé de stockage USB.

2.3 L'USB sans fil ?

Des projets consistant à porter des caractéristiques de l'USB au domaine du sans-fil tendent à apparaître, l'un en particulier étant déjà très médiatisé : le *Wireless USB* (s'appuyant sur la technologie `uwb`, *Ultra-Wideband*), lancé par un conglomérat de constructeurs, promet des produits commercialisés dans les mois à venir. Nous ne voulons pas nous étendre pour le moment sur cette nouvelle approche USB, mais il sera intéressant, en temps voulu, de vérifier si celle-ci permettra d'éviter les problèmes mentionnés dans les paragraphes suivants et si elle présentera des problèmes spécifiques.

2.4 Génération USB U3

Créée par la société U3 avec le soutien de constructeurs de mémoire flash, cette technologie transforme une clef USB en un système portable contenant des fichiers et des applications favorites.

Une clef USB U3 dispose d'un logiciel, ou `lanceur`, qui s'exécute sur l'ordinateur hôte afin de présenter (le plus souvent) les applications disponibles. Il est facile de gérer son contenu *via* un menu *"Démarrer"* (ou `lanceur`) dédié accessible dans la barre des tâches. Il est alors possible d'afficher à l'écran son *système* personnel sauvegardé sur la clef USB avec son fond d'écran et un accès facile aux différentes applications.

Les inconvénients de la gestion d'applications sur les clefs traditionnelles sont donc effacés : l'accès aux programmes se fait simplement et de manière transparente pour l'utilisateur ; s'appuyant sur un format qui cherche à se standardiser, l'offre logicielle compatible avec U3 ne cesse de se développer.

Autre caractéristique des clefs U3 : elles ne laissent que très peu de traces sur l'ordinateur hôte puisque les documents contenus sur la clef sont ouverts avec des applications elles aussi présentes sur la clef (y compris les cookies récoltés lors d'une navigation sur l'Internet). Les tâches d'écriture se font *via* la mémoire volatile de la machine hôte uniquement, et ces applications ne modifient ni la base de registre, ni la mémoire morte (ROM) de cette dernière.

De nombreuses applications gratuites ou payantes ont désormais des versions compatibles avec U3 : notamment le logiciel de voix sur IP Skype ou le navigateur Firefox. D'autres logiciels sont également disponibles : jeux, bureautique, gestionnaires d'images ou de fichiers audio MP3 ; et cette offre logicielle augmente de jour en jour.

L'USB U3 présente donc un avantage, pour la maîtrise de l'application utilisée ; par exemple, quand une personne est amenée à utiliser un ordinateur dont la configuration et le niveau de sécurité ne sont pas connus (comme dans un cyber-café, un hôtel, un aéroport, etc). Cela permet d'utiliser ses propres applications, plutôt que certaines méconnues, ou aux mises à jour et à la configuration non spécifiées. Elle reste cependant tributaire de la machine d'accueil

pour toute communication, toute saisie, et tout transfert de données vers l'extérieur, et cette opération peut l'exposer à certains risques décrits dans les paragraphes qui suivent.

3 Risques associés à l'USB

3.1 Vol d'informations de la clé

Une clé, ou tout autre support de stockage USB, est, une fois branchée sur une machine, à la merci de celle-ci. Un processus fonctionnant silencieusement, peut très bien attendre que la clé soit branchée (information signalée par le système d'exploitation) pour enclencher une procédure de lecture et de copie du contenu de la clé. Un tel processus, comme la plupart des codes malveillants actuels, ne sera pas facilement décelable sur la machine hôte (dissimulation au niveau de la liste des tâches, des appels système, etc.).

Certains outils plus pernicieux permettent même de faire une image complète de la clé. Outre le vol de documents présents dans celle-ci, ce procédé peut également faciliter la récupération de tout ou partie de documents effacés sur la clé.

Les clés disposent de voyants lumineux, montrant les échanges de données. Un clignotement anormal de la clé peut donc être une première indication d'une telle activité de copie. Attention cependant, le voyant peut aussi être manipulé de manière logicielle sur certaines clés. Quelques secondes suffisent enfin pour dérober plusieurs Mo de données avec les performances USB actuelles.

3.2 Exécution d'applications hébergées par la clé

L'action malveillante du paragraphe précédent est perpétrée par la machine d'accueil. Une autre approche, ou action malveillante, se nomme `podslurping` et s'effectue depuis le périphérique. Elle consiste à brancher sur un système un support de stockage, ou aussi un lecteur MP3 (`podslurping` fait référence au produit iPod d'Apple), afin d'en dérober furtivement de l'information.

L'ingénierie sociale, ou la force de persuasion, peut être associée à cette approche, afin de provoquer le branchement, et de perpétrer le vol des informations. Une phrase parmi les dialogues possibles pourrait être :

"Excusez-moi, pourrais-je connecter quelques minutes mon lecteur de musique MP3 sur votre port USB ?... Les batteries sont déchargées, et je ne rentre que demain chez moi. Merci beaucoup !".

Pendant quelques minutes, une partie du disque est copiée sur le lecteur de musique, qui dispose d'un espace de stockage important (de l'ordre de quelques Go à plusieurs dizaines de Go), et dont l'usage ne fait pas obligatoirement penser à un périphérique de stockage.

Ce scénario est aussi valable avec un appareil photo numérique.

Ce problème n'est absolument pas récent, et existait déjà à l'époque des disquettes. Cependant, les supports de stockage ont maintenant une capacité et un débit de transfert beaucoup plus importants, ce qui augmente la quantité de données pouvant être dérobées dans un cours intervalle de temps.

3.3 Problématique des clés USB U3

3.3.1 Mises à jour des logiciels

De nombreux scénarios d'attaques étudiés par le CERTA dans le cadre des incidents qu'il traite au quotidien sont dus à une absence de mises à jour, qui ouvre une brèche au niveau applicatif.

Il en va de même pour clés USB U3, dont le premier point délicat réside dans la maintenance des logiciels compatibles avec U3.

Ces logiciels, comme nous l'avons vu, sont pour la plupart des déclinaisons de ceux manipulés sur des systèmes plus standards (navigateur, client de messagerie, etc). En revanche, ils ont subi quelques modifications pour fonctionner sur le support U3, et quelques sites centralisent ces versions particulières.

Il se pose alors la question des mises à jour de ces dernières. Il n'est pas évident que les sites suivent de manière réactive les modifications des éditeurs officiels. Par ailleurs, la clé ne peut être mise à jour que si l'on dispose d'une connexion Internet.

Imaginons alors le scénario suivant :

1. l'utilisateur possède une clé U3, essentiellement pour un usage bureautique, afin de faire des présentations.
2. l'utilisateur branche sa clé régulièrement pour lire, rédiger et présenter des transparents.
3. la clé n'est pas mise à jour ; elle possède une version du logiciel de bureautique ayant des vulnérabilités permettant une exécution de code arbitraire par le biais d'un document spécialement conçu.
4. la clé peut servir à contaminer les ordinateurs sur lesquels les transparents sont visionnés.

Il est très délicat d'imposer aux utilisateurs d'une clé de se connecter à Internet pour effectuer les mises à jour. Ce n'est pas nécessairement l'usage premier qui est recherché.

Pour résumer, il existe les problèmes suivants, liés aux applications disponibles actuellement :

1. il n'existe pas de mise à jour automatique. Pour effectuer l'une d'elle, il faut supprimer l'application courante, afin d'installer une version plus récente ;
2. les applications compatibles avec U3 sont maintenues par certains sites, mais :
   - les éditeurs légitimes ne donnent généralement aucune garantie sur ces versions ;
   - les versions sont modifiées, et leur configuration est souvent criticable. Par exemple, l'installation d'un navigateur implique une page d'accueil spécifique, une barre de recherche pré-installée et méconnue, une configuration peu regardante sur la sécurité (taille du cache, activation du javascript), des favoris par défaut, etc.
   - certaines applications sont des espiogiciels, voire des troyens. Il peut aussi s'agir de jeux par exemple, compatibles avec U3, mais nécessitant au préalable un enregistrement *via* l'Internet (quel est le but de cette collecte d'information ?).
3. l'utilisateur doit régulièrement surveiller les sites, donc se connecter, pour découvrir les mises à jour.

Il reste possible de développer soi-même les versions de certaines applications (en faisant attention aux problèmes de licences). Plusieurs détails pour opérer se trouvent sur l'Internet, mais cela reste marginal, et nécessite à la fois des connaissances minimales pour compiler du code et une disponibilité des fichiers sources.

3.3.2 Vol d'informations

Compte tenu des applications disponibles, les clés U3 sont susceptibles de contenir des informations personnelles ou confidentielles :

- la configuration du client de messagerie ;
- les contacts stockés par le client de messagerie ;
- les pages en cache du navigateur Internet ;
- les sites favoris installés sur le navigateur ;
- des mots de passe gérés par une application dédiée (application fréquemment offerte par défaut avec la clé).

Le risque du vol de données comme il existe pour les clés classiques reste présent. Malheureusement, l'utilisation d'applications impose de fournir sur la clé U3 un minimum d'informations pour leur bon fonctionnement. D'autres applications U3 incitent également à centraliser des données confidentielles sur le support USB (gestionnaire de mots de passe par exemple). Le vol de celles-ci peut avoir des conséquences variées et génantes.

3.4 Les lanceurs malveillants

Pour finir, il faut noter que les clés U3 sont généralement fournies avec un `lanceur`, qui donne accès aux applications, une fois la clé insérée. Cependant, certains `lanceurs` malveillants sont également disponibles. Ils permettent d'exécuter directement des actions à l'insertion de la clé, et sont fournis avec des outils permettant : de récupérer les tables de mots de passe, d'installer une capture de clavier ou un `rootkit`, difficilement décelables *a posteriori*.

4 Les recommandations du CERTA

4.1 Comptes utilisateurs et droits

La clé ne dispose pas d'autres droits que ceux de l'utilisateur courant sous Windows. Pour limiter les actions que celle-ci peut effectuer sur le système, il est donc important de n'autoriser la connexion de clés que sur des sessions avec des droits limités, et de ne réserver les droits de l'administrateur qu'occasionnellement, pour la maintenance du système. Cette règle de base est également vraie, indépendamment des clés USB.

Sous Windows, pour ouvrir l'outil `Comptes d'utilisateurs`, il faut ouvrir le `Panneau de configuration` à partir du menu `Démarrer`, puis sélectionner `Comptes d'utilisateurs`. La gestion des comptes et des droits associés s'effectue à partir de cette interface.

4.2 Désactivation de la fonctionnalité `autorun`

Les clés U3 profite d'une propriété offerte par les systèmes d'exploitation Windows, nommée `autorun`. Elle consiste à exécuter automatiquement un logiciel lorsqu'un périphérique de stockage qui le contient est connecté. Microsoft autorise par défaut cette fonction pour le périphériques de type CDROM/DVDROM, ou les disques fixes.

Cette fonctionnalité est visible, quand, par exemple, à l'insertion de certains CD, une fenêtre de navigation Internet Explorer, ou une application d'installation s'ouvre. Un périphérique USB classique ne permet pas, lors de son insertion dans une machine fonctionnant sous Windows, d'exécuter automatiquement des programmes ou des commandes qu'il peut contenir. Dans l'objectif de faire exécuter automatiquement du code au cours de l'insertion d'un périphérique USB, certains fabriquants de matériels USB ont développé une astuce, qui consiste à faire passer celui-ci auprès de Windows pour un CD ou/et un DVD. Cette technique existe, et c'est elle qui est utilisée par les produits USB U3. Le principe général est que le périphérique, au moment de l'insertion, se présente comme un lecteur de CDROM USB, permettant *a fortiori* l'exécution d'un `autorun`.

La fonction `autorun` n'est généralement pas indispensable. Pour la désactiver sous Windows, il suffit de modifier la clé suivante dans la base de registres :

```
HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/CDRom
```

Pour la désactivation de l'`autorun` :

- Autorun = 0

pour l'activation de l'`autorun` :

- Autorun = 1

Cela fonctionne sur les systèmes Windows 95, Windows 98, Windows ME, Windows NT, Windows 2000, Windows XP et Windows 2003.

4.3 Verrouillage des postes

Afin d'éviter des incidents liés à l'insertion de clés USB sur son système, il est également important de verrouiller son poste de travail : sous Windows, cela peut se régler de manière automatique, après un manque d'activité de quelques minutes sur le système (choisir `Propriétés` après un clic droit sur le fond d'écran), ou de manière ponctuelle (appuyer simultanément sur les touches `Ctrl+Alt+Suppr` ou `Windows+L`).

L'insertion d'un périphérique USB sous Windows ne provoque pas son installation quand l'écran est verrouillé. La partition peut être cependant montée (`automount`) sous Linux malgré le verrouillage[2].

4.4 Clés USB de confiance : une clé par usage

Si une clé doit être insérée dans un système critique, il est important de vérifier son origine. Une solution serait de conserver une clé blanchie, régulièrement formatée, et de réserver l'usage de l'USB à cette seule dernière (ajout de nouveaux matériels/périphériques interdits). En d'autres termes, il faudrait considérer une clé par usage, voire interdire son déplacement hors des locaux liés à son utilisation.

4.5 Bloquer la clé en écriture

Certaines clés présentent un interrupteur physique, qui permet de bloquer l'accès en écriture à la clé. Il ne faut donc pas l'oublier. Si cela ne protège pas du vol d'information, et donc des différentes problématiques de confidentialité, cela empêche des éléments extérieurs de modifier le contenu de la clé, ou de l'effacer à

l'insu de l'utilisateur.

4.6 Nettoyer proprement le contenu de la clé

Les clés peuvent contenir des données sensibles. Avant de les prêter ou de les abandonner, il est important de bien nettoyer leur espace de stockage, ou d'assurer la confidentialité de leur contenu. En fonction des impératifs et des réglementations, certaines opérations doivent être conduites.

4.6.1 Mesures élémentaires

Il n'est souvent pas suffisant de faire `"supprimer"` pour détruire complétement toute trace d'un document. Des résidus peuvent subsister. Certains outils permettent de faire un nettoyage beaucoup plus complet.

- Sous Windows, il existe par exemple :
  - `eraser`

    http://www.bugbrother.com/eraser
  - `BCWipe`

    http://www.jetico.com/bcwipe.htm
- Sous Linux ou MacOS, il existe entre autres la commande `shred` (`Shredit` sous Mac OS) ou l'application :
  - `wipe`

    http://wipe.sourceforge.net/

Il faut cependant bien vérifier que tout l'espace de stockage reste inaccessible. Certains outils se contentent d'effacer des fichiers, mais d'autres temporaires peuvent encore subsister sur l'espace de stockage (cas des documents bureautiques avec Microsoft Word par exemple).

4.6.2 Mesures spécifiques

Dans le cas de données plus sensibles, il existe des mesures plus efficaces que celles précédentes. Elles peuvent s'appuyer sur des méthodes de surcharge, de démagnétisation, etc. Enfin, une dernière mesure consiste à détruire le support de stockage USB.

4.7 Chiffrement et intégrité

Nous n'aborderons pas ce point dans ce document, car les questions de chiffrement et d'intégrité se posent pour tout support de stockage, mais il est bien entendu que si la solution de chiffrement nécessite une clé, celle-ci ne doit pas se trouver sur l'appareil USB. De la même manière, le résultat du test d'intégrité ne doit pas être stocké sur le même support.

D'autre part, les clés actuelles offrent comme contrôle d'accès l'utilisation d'un mot de passe pour accéder aux fonctionnalités U3. C'est une première protection contre le vol, mais il faut garder à l'esprit que :

- si le mot de passe est frappé depuis une machine compromise (contenant une capture de frappe au clavier), ce dernier est récupérable. Or le CERTA observe

dans le cadre de traitements d'incidents que de tels outils malveillants sont fréquemment installés.
- le mot de passe est stocké sur le support amovible. Il peut donc être récupéré, sous une certaine forme, avec le reste des informations contenues (cf. le chapitre 3.1). Des tentatives de récupération par tests exhautifs reste possible, sans disposer de la clé en permanence.

5 Conclusions

Les périphériques de stockage USB offrent beaucoup d'avantages. Outre leur capacité importante, ils étendent actuellement leur champ d'action pour offrir à l'utilisateur des applications et des fonctionnalités multiples. Cependant, ces mêmes technologies peuvent également être utilisées à mauvais escient pour exécuter des actions malveillantes sur le système. *A contrario*, un système malveillant peut tirer profit de la qualité et la quantité des informations contenues sur ces supports, pour en dérober tout ou partie.

Il est important de considérer tout cela, pour un usage approprié de ces périphériques. Certaines mesures doivent être prises, selon le contexte, pour garantir un niveau de sécurité minimal. Etant donné l'usage répandu de ces appareils, un effort de sensibilisation est également nécessaire.

6 Documentation

- Caractéristiques de l'USB U3 :

  http://www.u3.com
- Comment désactiver la fonction autorun sur une machine Windows :

  http://support.microsoft.com/kb/q155217
- Site du standard USB :

  http://www.usb.org
- Documentation en français sur le fonctionnement de l'USB, par B. Acquier :

  http://acquier.developpez.com/cours/USB/
- Cours de Supélec par J. Weiss, "Le protocole USB' :

  http://www.rennes.supelec.fr/ren/fi/elec/docs/usb/usb.html

Gestion détaillée du document

09 novembre 2006
version initiale.
14 novembre 2006
corrections sur la forme.

Notes

... USB[1]
Le bus USB est l'interface matérielle, souvent incluse dans la carte mère d'un

ordinateur, permettant de relier l'unité centrale à un périphérique USB.
... verrouillage[2]
Cette opération est par exemple visible avec l'appel à la fonction `dasg`.

CERTA
2006-12-29

Navigation
Accueil
Accueil Privilèges
Jeu Boursier.com NEW
Broker online
22 Ordres
Cours de Bourse
PARIS
Cours en direct
Indices
Devises
Palmarès
Capitaux échangés
Cours de A à Z
DÉRIVÉS
Warrants
Certificats
Trackers
OPCVM
Sicav et FCP
NEW YORK
Indices US
Palmarès US
Françaises à NewYork
Infos & conseils
News - Paris
News - New York
News - Economie
Interviews
Rumeurs
Conseils Warrants
Introductions
Agenda
Communiqués presse
Accès Abonnés
Portefeuille Boursier
La reco du jour
Conseils Actions
Nos "exclus"
Nos stratégies
Avis des brokers
Valeurs opéables
SERVICES BOURSE
Services mobiles
Orange
SFR
Bouygues Tel.
Audiotel

Alcatel-Lucent — FR0000130007 - ALU

Ajouter à : ma liste mon portefeuille
Articles | Cours | Dérivés | Société | Graphique | Forum | Brokers | Analyse Tech
News | Conseils | Rumeurs | Interviews | Introduction | OST | Conseils warrants

Cotation du 18/05/2007 à 09h45

Dernier	Variation	Ouverture	Plus haut	Plus bas	Volume
9,91 €	+ 0,71 %	9,80 €	9,94 €	9,80 €	549 296

Chiffres
Capi. 22 889 M€
CA '05 13 135 M€
PER détail
RDT '06 1,61 %
Plus de chiffres
Informations
Place Paris
Marché MCA
SRD éligible
PEA éligible
Notre avis
11/05 PAYANT 9,98 €
24/04 PAYANT 9,05 €
26/03 PAYANT 8,67 €
05/03 PAYANT 9,20 €
09/02 PAYANT 10,42 €
Menu
Voir aussi
Toutes les news Paris
Options
Imprimer
Ajouter portefeuille
Ajouter à ma liste
Flash informations
09:58 - Reuters
Alain Juppé nommé numéro deux du gouvernement
09:55 - News
Marchés : le CAC se rapproche de ses meilleurs niveaux annuels
09:52 - News
Gouvernement : Jean-Louis Borloo nommé ministre de l'économie et de l'emploi
09:50 - News
Theolia : un application portant sur 0,53% du capital traitée
09:49 - News
Enel : feu vert du gouvernement espagnol à la montée dans Endesa
09:38 - News
Sorefico Coiffure : en croissance de 4,4% au premier trimestre
09:35 - News
AstraZeneca : feu vert de la FDA à

News

Alcatel-Lucent : un disque de données salariés de Lucent envolé

18/05/2007 - 08h55 | aucun commentaire dans le forum DIVERS

(Boursier.com) - Voilà une affaire qui ne devrait pas avoir de retentissements financiers, mais qui n'arrange pas vraiment l'image du groupe aux Etats-Unis. Alcatel-Lucent a annoncé cette nuit avoir été informé le 7 mai par un prestataire qu'un disque dur contenant des informations personnelles avait été perdu. Le disque contient notamment toutes les données (nom, adresse, numéro de sécurité sociale, salaires, pensions) de salariés actuels et retraités américains de Lucent ainsi que de leurs ayant-droits. Il ne comprend pas en revanche de données comme les numéros de carte de crédit ou les mots de passe.

Le disque disparu avait été préparé par Hewitt Associates pour livraison par UPS à Aon Corporation. Il s'est évaporé ou a été volé lors de son transfert, soit entre le 5 avril et le 3 mai. Alcatel-Lucent a averti les autorités fédérales américaines qui ont ouvert une enquête, et mène en parallèle en interne ses propres investigations. Le groupe assume sa part de responsabilité dans cette disparition et assure les personnes figurant dans le fichier qu'il fera tout pour minimiser la portée de sa disparition.

A.B.

Soyez le premier à réagir à cet article !
Ajouter un commentaire
Les news précédentes

Accueil
Rubriques
Technologie
Economie IT
Développement
Solutions PME
SSII
Emploi/Formation
Micro
Numérique
Agenda
Vidéos
Thèmes
LMI Blogs
Téléchargements
Conférences
Forums
Newsletters
Flux RSS
Zone Directe
Livres Blancs

Sécurité
Inscrivez-vous XML
Consulter le centre de compétences

Version imprimable | Envoyer à un ami | Recevez les news

Les services informatiques, premiers responsables des fuites de données

Edition du 05/12/2007 - par Marie Calzergues

Selon une étude du cabinet Orthus, 30 % des fuites de données sensibles trouvent leurs origines dans le service informatique de l'entreprise. Et elles auraient toutes pu être évitées en appliquant le règlement intérieur des sociétés.

Après plus de 100 000 heures d'activité supervisées, le verdict d'Orthus, un cabinet britannique spécialisé dans la sécurité, est tombé. Les services informatiques sont les principaux responsables des fuites de données (à 30 %) devant les services clients à 22 %. Pour Richard Hollis, directeur d'Orthus : « Cette étude confirme la règle : plus les droits d'accès sont élevés, plus la tentation d'en abuser est grande. Les sociétés doivent considérer l'espion interne comme la première menace pour leurs affaires. Sans cela, aucune sécurité réelle ne peut être atteinte. » De plus, l'enquête a prouvé que dans 68 % des cas, des appareils mobiles (portables, PDA, smartphones, voire des baladeurs MP3 ou des clés USB) ont été utilisés. Parmi les autres outils privilégiés pour la fuite de données se trouvent les webmail, les réseaux sociaux et les logiciels de messagerie instantanée. Dans tous les cas observés, une application plus stricte des règles de sécurité internes auraient suffi à éviter ces fuites.
Cette enquête a été menée en installant des « mouchards » sur les postes de travail et les serveurs des entreprises impliquées, qui ont fourni une liste de mots-clés et de fichiers sensibles spécifiques à leur activité.

En savoir plus
Le site d'Orthus

Rejoignez lemondeinformatique.fr, commentez cet article
Nombre de commentaires postés (0) - Lire tous les commentaires

Pour commenter cet article inscrivez vous ou identifiez vous ci-dessous si vous êtes déjà inscrit :

Email :
Mot de passe : oublié ?
Mémoriser mes identifiants
OK

L'ACTUALITÉ DU JOUR

OPEN SOURCE
Verizon attaqué pour non respect de la GPL
(10/12/2007 12:50) - Les défenseurs des logiciels libres n'hésitent plus à se défendre devant les tribunaux. (...)

FORMATION
Le correspondant informatique et libertés entre à l'université
(10/12/2007 11:42) - Les universités de l'Hexagone viennent d'annoncer la création d'un réseau de correspondants (...)

SÉCURITÉ
Les 10 « pertes de données » les plus surprenantes de l'année
(10/12/2007 10:33) - Décembre est l'heure des bilans et l'informatique n'y échappe pas. D'autant que certains (...)

STOCKAGE
Seagate rachète un spécialiste de la recherche de preuves
(10/12/2007 10:07) - Le fabricant de disques durs Seagate Technology vient de racheter son compatriote (...)

OPEN SOURCE
La Région Ile de France adhère à l'Adullact
(07/12/2007 17:56) - L'Association des Développeurs et des Utilisateurs de Logiciels Libres pour les Administrations (...)

PÉRIPHÉRIQUES
Explosion de la demande en capacité de stockage externe
(07/12/2007 16:57) - Que se passe-t-il ? Au troisième trimestre, IDC a constaté une hausse exceptionnelle (...)

Articles récents SÉCURITÉ

Les 10 « pertes de données » les plus surprenantes de l'année
(10/12/2007 10:33) - Décembre est l'heure des bilans et l'informatique n'y échappe pas. D'autant que certains (...)

Microsoft terminera l'année avec sept correctifs dont trois sensibles

Sondage flash
Pour vos contrats, vous préférez
Un gros acteur pour l'assurance de tout trouver
Privilégier les acteurs locaux et/ou indépendants
Panacher votre panier selon vos besoins
Voter

LMI Vidéo
> Les Entretiens
> Les Webcasts
> Les Reportages

Conférences
29/01/2008
MOBILITE
De 8h30 à 14h00 à l'Automobile Club de France - Paris 8è
s'inscrire
toutes les conférences

Agenda
Du samedi 15 décembre 2007 au samedi 15 décembre 2007
Cap'Tronic 2007
Sélestat (67)
en savoir plus
tout l'agenda

Réseaux-Télécom.net

L'humain reste le maillon faible de la sécurité du SI

Edition du 24/09/2007 - par Marie Caizerques

Dans son rapport annuel « 2007 Global Security Survey », le cabinet Deloitte Touche Tomatsu montre que les employés et les clients restent le plus grand facteur de risque d'une institution financière.

Mené auprès de 169 institutions financières dans le monde, le sondage « 2007 Global Security Survey » du cabinet Deloitte Touche Tomastu (DTT) montre que le facteur humain (employés, clients ou partenaires) reste la faille principale dans la sécurité des systèmes informatiques. Quelque 65 % des entreprises interrogées ont subi au moins une attaque l'an dernier provenant soit de l'intérieur (pour 31 % d'entre elles), soit de l'extérieur (pour 65 % d'entre elles). Les attaques de l'intérieur proviennent de mauvaises manipulations de la part des employés qu'elles soient intentionnelles, ou résultant d'erreurs ou d'ignorance.

Un paradoxe sécuritaire

Si cela inquiète 91 % des participants au sondage, bien peu essaient toutefois d'y remédier. Seules 63 % des institutions financières interrogées disposent d'une stratégie d'information sur la sécurité. Et 22 % d'entre elles n'ont fourni aucune formation à leurs employés sur la sécurité en un an. Du coup, seulement 30 % des sociétés interrogées estiment que leurs employés ont les compétences nécessaires pour faire face à des problèmes de sécurité. « Ces résultats contradictoires soulignent le paradoxe sécuritaire auquel sont confrontées les institutions financières », affirme Adel Melek, dirigeant du groupe sur la gestion des risques et de la sécurité au sein de DTT. « D'un côté, il est clair que les répondants ont identifié les principaux risques et les mesures à prendre pour améliorer leur sécurité. Et de l'autre, de nombreuses organisations financières sont en retard pour mettre ces mesures en place. »

Si les employés représentent un risque majeur, ils ne sont pas les seuls. Les clients des institutions financières restent le risque principal. Ils sont en effet le vecteur privilégié par les cyber-criminels pour mener les trois principales attaques menaçant des institutions financières : virus et vers, spams et phishing. Pour opposer un barrage efficace, la sécurité se heurte à un impératif commercial et au travail de titan que cela représenteraient.
66 % des sociétés interrogées se refusent à tenir leurs clients responsables de ces attaques, et à se sentir concernés par d'éventuelles failles de sécurité sur les ordinateurs de leurs clients.

En savoir plus
Global Security Survey 2007

Url :
http://www.reseaux-telecoms.net/actualites/lire-l-humain-reste-le-maillon-faible-de-la-securite-du-s

Mobilegov, Spin-off du projet européen eJustice (développement des technologies pour la mise en place de la carte d'identité biométrique - www.ejustice.eu.com), a été créée en 2004 en France et au Royaume-Uni.

Mobilegov sait détecter, par des moyens logiciels, toute modification (hard ou soft) dans un système informatique. Sa technologie est brevetée en Europe et aux USA. Alors que pour beaucoup d'entreprises, la sécurité se résume à interdire l'usage de périphériques potentiellement dangereux, par exemple en bloquant les ports USB au détriment de l'efficacité, Mobilegov vous permet d'utiliser les outils les plus performants, mais de façon contrôlée et personnalisée en fonction des besoins des collaborateurs.

Mobilegov répond de façon unique aux problèmes du vol de données dans les entreprises en proposant d'étendre la sécurité du réseau d'entreprise aux périphériques à mémoire (clés uSB, disques, graveurs, etc.), empêchant l'utilisation d'un périphérique hors de l'entreprise.

Link Resource

Mobilegov

TVEP

Mobilegov opens an office in the 'UK Silicon Valley'

French security software editor Mobilegov launches its UK presence this autumn in Reading at the heart of the Thames Valley following several months of market research and supported by the Thames Valley Economic Partnership (TVEP), South East England Development Agency (SEEDA) and UK Trade & Investment (UKTI) in Paris.

A strategic location

Mobilegov is a French company developing original and patented software to protect companies and organisations against the threat from the use of unauthorised equipment (PDAs, Smartphones, USB sticks, external and internal drives etc.). At this stage the company has two main solution offerings, Device Authenticator which protects networks against the use of unwanted removable media devices and Device Linker which allows the use of USB sticks only on authorised configurations. Mobilegov is a global player in Data Loss Prevention helping companies to protect their main asset - their data. Mobilegov has opened an office in GreenPark, Reading next to companies such as Cisco, Symantec and LogicaCMG. Managing Director François-Pierre Le Page has spent much time searching for the ideal location for its UK centre.

"As a leading patented technology owner, we were very strongly encouraged by SEEDA and TVEP to setup in the UK. The fact that Sophia Antipolis, where we have our Head Office, has many similarities with the Thames Valley (Large ICT Community) made our choice easier. We have built a fantastic link between local Government agencies and, at the same time, it is crucial for the development of our network to stay close to our resellers and partners"

Mobilegov has built a significant and impressive network of partners in Europe and starts its operations in the UK with LogicaCMG. The company is supported by the French Government and its solutions are used by organisations within diverse markets such as Military & Defence, Nuclear and Energy, Universities and R&D centres.

Ben Churchill, TVEP's Inward Investment Manager said "We are delighted to welcome MobileGov to the Thames Valley, where it can enjoy the company of some of the world's leading IT companies and join a business community that strongly supports and encourages innovation. MobileGov is ideally placed to develop its position as a technology leader and to engage with new partners and customers in the UK".

Laetitia Régnault, SEEDA's Director of Business Development in France said that "MobileGov's dynamism and confidence to expand into new markets made our job of supporting them by creating introductions and helping build key relationships a pleasure and contributed greatly to their successful arrival in the UK".

About Mobilegov

Mobilegov is a French security software editor providing hardware identification solutions, device access management solutions and USB storage devices having the capacity to recognise the configurations they are connected to. All the Mobilegov solutions are patented. The solutions are distributed by a network of international resellers and Integrators and protect companies and organisations of any size. Mobilegov is a private company, founded in 2004 with its head office in Sophia Antipolis, the French Technopole.

Device Linker, la clé USB sécurisée - Source : zebulon.fr

Par Yann - publié le 30/07/2007 à 14h31

Les clés USB ont depuis bien longtemps pris une place prépondérante dans notre quotidien. Pourtant, en cas de perte ou de vol, nos précieuses données peuvent se retrouver entre de mauvaises mains. De plus, en ce qui concerne les entreprises ou les administrations publiques, ces clés introduisent une nouvelle menace de sécurité où des données confidentielles peuvent facilement être dérobées. Face à ce constat, la société Mobilegov propose une clé USB sécurisée utilisable uniquement sur des PC autorisés. Nous sommes donc allé à la rencontre de cette société afin de pouvoir tester en conditions réelles cette solution de stockage sécurisée.

Introduction

Les clés USB permettent aujourd'hui à tout un chacun de transporter ou échanger facilement ses fichiers, que ce soit des photos de ses dernières vacances ou encore des données confidentielles de première importance. Mais quelque soit le type d'informations contenues sur la clé, sa perte ou son vol peut être problématique.

De même, la prolifération des périphériques de stockage amovible tels que les clés USB, PDA, baladeurs audio ou encore téléphones portables constituent une nouvelle menace de sécurité dans les entreprises où un collaborateur mal intentionné peut voler des données confidentielles sur un support amovible.

Pour contrer ces problèmes de sécurité, il existe différents moyens de protéger les données d'une clé USB. On trouve ainsi des clés intégrant un encryptage matériel AES 128 bits où les données sont cryptées "à la volée". D'autres constructeurs se sont quant à eux tournés vers des clés biométriques. Là encore, les données se voient cryptées et votre empreinte digitale fait alors office de mot de passe.

Si de telles solutions sont très efficaces en cas de perte où de vol de la clé, elles ne répondent pas à la problématique rencontrée par les entreprises : la fuite de données sensibles à l'extérieur de la société.

La solution proposée par *Mobilegov*, **Device Linker**, permet de contrer cette double problématique : en cas de perte ou de vol, les données seront protégées et la fuite des données à l'extérieur sera rendue impossible.

Nous avons donc rencontrés les dirigeants de *Mobilegov* afin de pouvoir tester la solution Device Linker. Nous avons effectué notre test avec la version de 512 Mo qui est proposée au prix de 29.90€.

javascript:ShowPopup('/pop-image.php?pic=http://www.zebulon.fr/images/dossiers/device-linker/device-lir

La clé en elle même est tout ce qu'il y a de plus classique et adopte un look plutôt élégant avec une partie en plastique transparent qui laisse apparaître les composants internes et une autre partie en aluminium légèrement brossé du meilleur effet. A noter que le périphérique existe également en version 1Go, 2Go, 4Go et 8Go. Enfin, quelque soit la capacité de la clé, le système de protection utilisé reste le même.

Une clé USB U3

La technologie du Device Linker repose sur la plateforme U3. Avant de voir plus en détail le fonctionnement de la clé de *Mobilgov*, intéressons-nous tout d'abord à l'U3. La plate-forme U3 permet de transformer une clé USB en un véritable bureau virtuel pouvant contenir à la fois des documents classiques mais aussi différentes applications directement utilisables sur le support amovible.

L'U3 est donc un standard créé par la société du même nom. Si à l'origine seules deux sociétés (Scandisk et M-Systems) soutenaient cette initiative, de nombreux autres constructeurs utilisent aujourd'hui la licence U3 afin de proposer des clés USB U3.

Une clé U3 permet donc de transporter aussi bien des données, tout comme le fait une clé USB classique, mais aussi des applications avec leurs paramètres de configuration. Ainsi, un client email conservera ses informations de connexion au serveur email distant et un navigateur web possèdera ses favoris.

Le principe de fonctionnement d'une clé U3 est extrêmement simple : dès son insertion, une interface appelée *Launchpad* est automatiquement exécutée. Cette application, ressemblant à s'y méprendre au menu démarrer de Windows XP, permet de lancer toutes les applications présente sur la clé U3. La partie de droite de Launchpad quant à elle, permet de gérer les applications de la clé.

Concrètement, une clé U3 possède deux partitions : la première, correspondant à une partition

CD-ROM (en lecture seule), contient l'application qui se lancera automatiquement lors de l'insertion de la clé. La seconde partition quant à elle, est privée et protégée par mot de passe. Il existe de nombreuses applications compatibles U3. Ces dernières, facilement reconnaissables car portant l'extension .u3p, sont regroupées sur cette page (http://software.u3.com/) sur le site de l'U3.

Enfin, pour plus de sécurité, chacune des applications créera automatiquement son espace de stockage temporaire sur la clé. Si celle-ci venait à être retirée de la machine, cet espace serait automatiquement effacé.

La technologie utilisée par Mobilegov pour la clé Device Linker prend donc place sur un support U3. Voyons ensemble le principe de fonctionnement de cette clé sécurisée.

Principe de fonctionnement et installation

Le principe théorique de fonctionnement de la clé Device Linker est très simple. Dès l'insertion de la clé, cette dernière va vérifier si la machine utilisée est autorisée. Si oui, l'accès aux données contenues sur la clé sera alors possible. Dans le cas contraire, l'accès sera interdit.

Dès la première insertion de la clé Device Linker, le Launcher U3 s'exécute. En explorant la partition de données de la clé, nous avons les fichiers suivants :

Un double clic sur *DeviceLinkerSetup1_0_Single.msi* permet de lancer l'installation. Cette dernière est tout à fait classique et se déroule sans encombre.

Une fois l'installation terminée, il vous sera nécessaire d'indiquer votre identifiant et le numéro de série correspondant.

Ces informations sont présente dans l'emballage de la clé et sont visibles uniquement après avoir ouvert le blister du Device Linker. Nous avons testé ici la *Single Edition* du Device Linker, l'identifiant que nous indiquons ici est unique. Si cette version est plutôt orientée vers les particuliers, il existe néanmoins une version destinée aux entreprises. Dans ce cas, seul le logiciel est fourni. L'ensemble des clés U3 existantes est alors compatible.

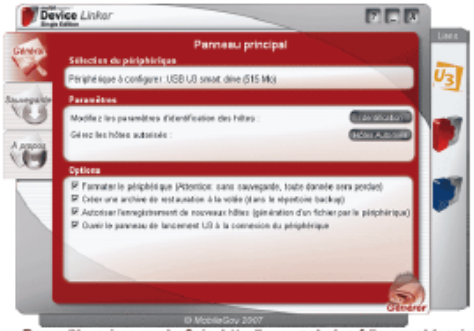
Initialisation du Device linker

Après l'insertion de la clé dans l'ordinateur, cette dernière est automatiquement reconnue et son initialisation commence.

Un double clic sur l'icône du programme va alors nous permettre de configurer la clé USB.

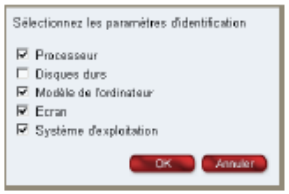
Cette étape permettra à la partie logicielle de fonctionner avec notre clé U3.

La fenêtre principale de l'application permet l'identification et la gestion des hôtes, c'est à dire des ordinateurs qui auront la possibilité d'accéder au contenu protégé de la clé U3.



(javascript:ShowPopup('/pop-image.php?pic=http://www.zebulon.fr/images/dossiers/device-linker/gen

La configuration de la méthode d'authentification est très simple. Un clic sur le bouton *Identification* permet de sélectionner les éléments de son choix.



Comme nous le voyons, il y a différents paramètres d'identification possible : processeurs, disques durs, modèle d'ordinateur, écran et système d'exploitation. Ces différents éléments seront alors utilisés pour générer (de façon transparente) un identifiant unique correspondant à la machine. Ainsi, le PC hôte pourra par la suite être reconnu et identifié.

Plus le nombre d'éléments pris en compte est important, plus l'identification sera fiable. Il reste néanmoins possible de ne pas prendre en compte certains éléments de la configuration en décochant ceux de son choix. Cela permettra par exemple de ne pas avoir à générer une nouvelle identification de son périphérique si vous changez régulièrement de disque dur ou de système d'exploitation. Cela peut également être utile dans le cas de parc informatique important où l'on peut planifier à l'avance les upgrades des machines en sachant quels éléments seront changés ou non.

Ensuite, il ne nous reste plus qu'à configurer la clé avec les éléments nous venons de choisir en cliquant sur le bouton *Générer* en bas à droite de la fenêtre de l'application.

(javascript:ShowPopup('/pop-image.php?pic=http://www.zebulon.fr/images/dossiers/device-linker/gen

Le programme nous rappelle alors les différents paramètres d'identification des hôtes que nous avons choisi ainsi que les machines autorisées à accéder à la clé. Un clic sur le bouton *Lancer* permet alors la génération de la clé qui prendra quelques secondes (voir minutes en fonction de la puissance de la machine).

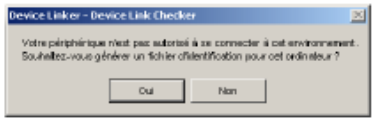
Une fois la configuration de la clé terminée, vous pouvez la retirer. Le contenu de la partition cryptée sera alors accessible uniquement sur notre machine.

Gestion des hôtes

Toujours dans la fenêtre principale de l'application, il est possible de consulter les hôtes autorisés. Un simple clic sur le bouton correspondant permet de sélectionner les machines pour pourront accéder au contenu de la clé :

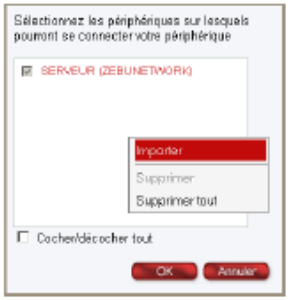
Par défaut, seule la machine sur laquelle l'application a été installé est autorisé. La machine principale (le "*Master Host*") est ici indiquée en rouge. C'est cette machine qui va gérer les autorisations de la clé. Il est bien entendu possible d'ajouter d'autres machines par la suite de façon très simple : l'insertion de la clé U3 sur un autre PC va automatiquement proposer la création d'une nouvelle identification.

Ainsi, lors de l'insertion de la clé sur une machine inconnue, la fenêtre suivante apparaîtra :



Si vous acceptez, un fichier ayant pour extension *.qki* sera automatiquement généré. Pour autoriser la machine, il faut ensuite rapatrier le fichier *.qki* sur la machine principale. Ce rapatriement du fichier d'identification peut se faire par email, réseau ou à l'aide d'un autre équipement de stockage. On ne peut bien entendu pas encore utiliser notre clé U3 car celle-ci n'étant pas encore autorisé, il n'est pas possible d'y copier un quelconque fichier.

Sur le poste maître, il est maintenant possible d'importer simplement le fichier d'identification en effectuant un clic droit dans la fenêtre de gestion des hôtes. Dans le menu contextuel qui apparaît, il suffit simplement de choisir l'option *Importer* puis, à l'aide d'un bouton parcourir, d'aller chercher le fichier d'identification généré par notre machine inconnue.

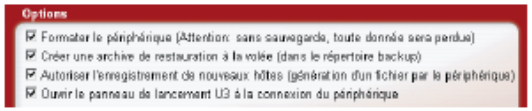


Après avoir ajouté la (ou les) machine(s) autorisée(s), il suffit simplement de régénérer la clé pour que celle-ci soit acceptée sur les nouveaux hôtes.

Sauvegarde, restauration et options

L'interface de gestion de la clé propose également différentes options ainsi que la possibilité de créer une sauvegarde du contenu de la clé. En cas de perte, il sera donc toujours possible de créer une nouvelle clé à partir de notre machine principale.

Les options disponibles sont les suivantes :



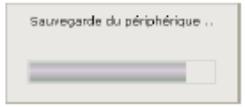
Il est donc possible de formater la clé, de créer une sauvegarde automatique lors des générations, d'autoriser l'enregistrement de nouveaux hôtes ou encore de lancer ou non le *LauchPad* lors de l'insertion de la clé.

A noter que si l'on n'autorise pas la création de nouveaux hôtes, aucune demande d'identification de sera effectuée lors de l'insertion de la clé sur une machine inconnue.

Enfin, pour sauvegarder l'ensemble de données contenues sur la clé, il suffit simplement d'aller dans l'onglet *Sauvegarde* de l'application.

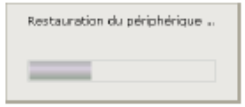
(javascript:ShowPopup('/pop-image.php?pic=http://www.zebulon.fr/images/dossiers/device-linker/sau

Après avoir choisi le chemin et le nom du fichier de sauvegarde, un clic sur le bouton *Sauver* lance la sauvegarde des données.



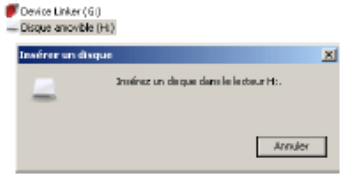
Le fichier généré sera une simple archive au format .zip.

Concernant la restauration, il suffit d'aller sélectionner une archive de sauvegarde sur notre disque dur puis de cliquer sur le bouton *Restaurer* afin que l'arborescence complète et les fichiers soient restaurés sur la clé.



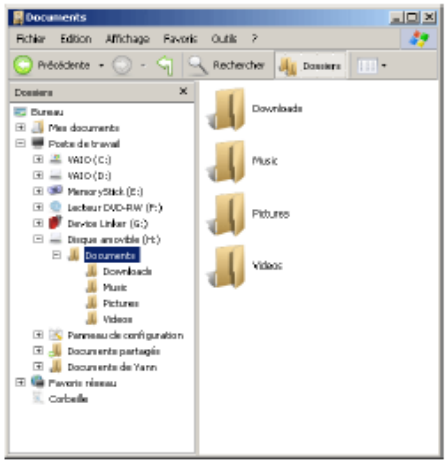
Conclusion

Si le principe de la clé Device Linker est simple en théorie, son fonctionnement l'est tout autant dans la pratique. Ainsi, lors de l'insertion de la clé sur une machine inconnue, nous n'avons pas pu accéder à la partition de donnée.



Si la clé est bien détectée et que la partition en lecture seule est visible, la seconde partition de la clé U3 est inaccessible. Windows la reconnaît comme un lecteur dans lequel aucun disque n'aurait été inséré.

Après avoir régénéré le périphérique en y ajoutant l'identification de notre nouvelle machine, l'insertion de la clé laisse apparaître l'ensemble du contenu de la seconde partition.



Cette partition est bien entendu accessible en lecture et écriture.

Pour le particulier, la version *Single Edition* permettra de protéger efficacement ses données contre la perte ou le vol en toute simplicité. Après avoir autorisé sa (ou ses) machine(s), l'utilisation de la clé sera totalement transparente. Le point fort du système est qu'il ne sera pas nécessaire pour l'utilisateur de mémoriser un quelconque mot de passe puisque celui-ci est généré automatiquement et reste inconnu de l'utilisateur. Tout se fait de façon transparente et en toute simplicité.

Pour l'entreprise, le bénéfice est double si la logique de sécurité réseau est respectée. Non seulement les données sont protégées contre la perte ou le vol mais toute tentative de fuite de données par un collaborateur peu scrupuleux est interdite. Bien sûr, rien n'empêche alors l'utilisation d'une clé USB classique pour récupérer des données confidentielles. Dans ce cas, il est alors nécessaire d'utiliser la solution *Device Authenticator* conjointement à Device Linker. Cette solution, que nous n'avons pas testée, permet de gérer tous les équipements se connectant à un réseau d'entreprise. Ainsi, un périphérique non autorisé ne pourra fonctionner sur une machine donnée. En interdisant alors l'utilisation des autres périphériques de stockage externe, le réseau est donc protégé contre la fuite de données.

Pour conclure, nous avons été séduit par le fonctionnement du Device Linker. Les données sont protégés de façon simple et efficace et surtout, de façon totalement transparente. Une fois nos différentes machines autorisées, on oublie que nous avons entre les mains une clé où nos données sont en sécurité !

Nous pouvons par contre distinguer deux bémols : tout d'abord, la clé ne fonctionne que sous Windows XP. Si l'on peut se douter qu'une telle solution ne soit pas multi plateforme, on regrette toutefois l'absence du support de Vista. Même s'il ne s'agit pas d'un besoin urgent

pour les entreprises, Windows Vista commence petit à petit à s'implanter dans les foyers. Fort heureusement, le fonctionnement de Device Linker est prévu sous cet OS pour 2008.

Enfin, le type même du fonctionnement de la clé oblige l'utilisateur à repasser par le poste maître pour gérer les autorisations. Si ce principe de fonctionnement est tout à fait logique, il peut empêcher l'utilisation de la clé si vous n'avez pas accès au poste maître pour ajouter l'identification de la nouvelle machine.

Malgré ces deux éléments gênants, force est de reconnaître que le Device Linker fonctionne très bien. Sa technologie (qui est brevetée) permettant d'identifier une machine fonctionne à merveille, la distinction des équipements se faisant de manière totalement unique. Même deux configurations exactement similaires seront différenciées. C'est là une alternative originale et efficace face aux autres clés USB sécurisées du marché.

Pour plus d'informations, vous pouvez consulter le site Device Linker (http://www.devicelinker.com/) de Mobilegov.

Source : Zebulon.fr (http://www.zebulon.fr/dossiers/78-cle-usb-securisee-device-linker.html)

Réseaux-Télécom.net

La cybercriminalité se professionnalise

Edition du 21/09/2007 - par Eddye Dibar

Selon le dernier *Rapport sur les menaces à la sécurité Internet* publié par Symantec, la cybercriminalité devient une activité de plus en plus professionnelle et commerciale. Les pirates et autres organisations criminelles cherchent à tirer toujours plus de profit de leurs attaques en ligne. Aujourd'hui elles n'hésitent pas à développer leurs propres réseaux de pirates. « Les dernières observations de Symantec montrent que le cybercriminel d'aujourd'hui est extrêmement compétent et intelligent », explique Lee Sharrocks, directeur commercial grand public de Symantec au Royaume-Uni.

D'autant que des outils simples et clés en main circulent sur le Web. Conçus par des cybercriminels, ces kits quasi *plug and play* sont vendus entre 35 et 75 euros et permettent même à des personnes non expérimentées d'organiser, en quelques clics, des campagnes de phishing par exemple.

Depuis plusieurs semaines, l'éditeur de solutions de sécurité recense un nombre croissant de serveurs commerciaux clandestins. Ces plates-formes permettent aux pirates de vendre et d'acheter tout type d'information susceptible d'être monnayée : cartes de crédits, comptes bancaires, mots de passe de boîtes électroniques, etc (voir encadré).

Au cours du premier semestre 2007, les Etats-Unis hébergeaient le plus grand nombre de serveurs commerciaux clandestins, avec 64% du total identifié par Symantec. « L'Internet clandestin se développe à une vitesse inquiétante », alarme Lee Sharrocks. Selon les dernières tendances le nombre de sites d'enchères au marché noir continue d'augmenter. « Il s'agit d'un marché illégal de plusieurs milliards de dollars », conclut-il.

Répartition des articles mis en vente sur les serveurs commerciaux clandestins

Rang	Article	% de tous les articles proposés	Prix moyen
1	Cartes de crédit	22 %	0,35€ - 3,62€
2	Comptes bancaires	21 %	22€ - 290€
3	Mots de passes de boites e-mail	8 %	0,73€ - 254€
4	Mailers	8 %	5,8€ - 7,3€
5	Adresses e-mails	6 %	1,4€/Mo - 2,9€/Mo
6	Proxies	6 %	0,35€ - 2€
7	Identités complètes	6 %	7,3€ - 108€
8	Scams	6 %	7,3€/semaine
9	N° de sécurité sociale	3 %	3,6€ - 5€
10	Shells sous Unix	2 %	1,4€ - 7,3€

Source: Symantec Corporation

Url :
http://www.reseaux-telecoms.net/actualites/lire-la-cybercriminalite-se-professionnalise-17147.html

Mon panier Téléchargement
Votre panier est vide

Téléchargement de logiciels

Actualités
Nouveautés
Affaires de Fnac

Catégories
Arts et culture
Bureautique
Educatif
Internet
Jeux détente
Jeux enfants
Jeux Vidéo
Loisirs / Vie Pratique
Multimédia
Sécurité
Traduction
Utilitaires

Services Fnac
» Aide au téléchargement
» Extension de téléchargement
» Conditions générales de vente

nexway
www.nexway.fr

Rechercher | Logiciels à télécharger | OK

Accueil >> Téléchargement de logiciels >> Sécurité >> Sauvegarde

Device Linker - single soft

Device Linker® vous protège contre le vol de vos données sauvegardées sur votre clé U3 en cas de perte ou de vol. Tant que votre clé USB U3 ne reconnaît pas la configuration sur laquelle elle est connectée, elle reste inutilisable et l'accès aux données qu'elle contient est impossible !

Editeur : MOBILE GOV
En téléchargement

Durée de téléchargement -512Ko / 07mn -2Mo / 01mn -8Mo / 00mn

29.90 €

Disponibilité immédiate

Télécharger ce logiciel

En détail | Configuration

Description

Pour que vos périphériquesde stockage de données ne fonctionnent que sur vos machines !

Device Linker® vous protège contre le vol de vos données sauvegardées sur votre clé U3 en cas de perte ou de vol. Tant que votre clé USB U3 ne reconnaît pas la configuration sur laquelle elle est connectée, elle reste inutilisable et l'accès aux données qu'elle contient est impossible ! Device Linker® ne nécessite aucune modification de votre environnement informatique.

Protégez-vous contre :

L'UTILISATION DE VOS PERIPHERIQUES USB U3 SUR DES PCs NON AUTORISES
La technologie Linker® rend vos périphériques USB U3 inutilisables en dehors de l'environnement que vous choisissez (réseau de l'entreprise, pool de machines).

LA PERTE OU LE VOL DE VOS CLES USB U3
La clé USB reste inaccessible tant qu'elle ne reconnaît pas l'ordinateur sur lequel celle-ci est connectée. Device Linker® ne nécessite aucune modification de votre environnement informatique. La protection s'applique à tous les périphériques U3 existants.
Une interface d'administration simple vous permet de configurer vos périphériques et les hôtes sur lesquels ils fonctionneront.

Principales fonctionnalités :

Définition dynamique des environnements : sélection des paramètres d'identification d'une machine hôte à partir d'une liste préétablie (CPU/ OS/ cartes mère/ etc.).

Gestion des machines hôtes : enregistrement direct sur une machine non identifiée et gestion des listes de machines autorisées.

Enregistrement des modifications sur la clé et gestion transparente et sécurisée (mot de passe généré inconnu de l'utilisateur) d'une partition chiffrée et cachée.

Options de backup et de restauration des clés

Peut s'utiliser conjointement avec Device Authenticator® les clés Device Linker pouvant ainsi être intégrés à la logique de sécurité réseau.

Comment fonctionne Device Linker®

1. Au cours d'une première étape de configuration, le périphérique est connecté à n'importe quel PC du Réseau afin de définir l'environnement sur lequel il pourra être utilisé : ce PC, un groupe de PC, le LAN sur lequel le PC est lui-même connecté.

2. Il faut ensuite définir les mesures à prendre si le périphérique est connecté à un environnement imprévu : rendre le périphérique illisible, transmettre discrètement des informations sur l'environnement, détruire les données ou demander une autorisation d'usage temporaire.

Principaux matériels compatibles :
Certifié U3, Device Linker® reconnaît les matériels informatiques USB U3

Configuration requise :

- OS : Windows 2000/2003/XP/VISTA (administration sous XP)
- Processeur : Pentium II
- Espace disque dur : 40 Mo d'espace libre
- Mémoire vive : 256 Mo RAM

[SÉCURITÉ]

L' « ADN numérique » des périphériques sécurise leurs connexions

Mobilegov propose une solution de gestion de la sécurité des équipements amovibles, dont les smartphones et les clés USB.

Gilbert Kallenborn , 01net., le 20/12/2007 à 15h55

Avec Device Authenticator Pro Edition (DAPE), la jeune pousse française Mobilegov fournit une solution élégante à un problème qui prend de l'importance en entreprise : la gestion des périphériques amovibles. Ces équipements sont de plus en plus sophistiqués et donc difficiles à contrôler.

Clé USB, smartphone dernier cri ou simple iPod, tous peuvent servir au vol de données ou à la corruption du système d'information. *« En particulier, les clés USB U3, qui sont dotées d'un véritable microprocesseur, sèment la terreur dans les bureaux, car elles permettent de lancer des applications sans que le service informatique ne s'en rende compte »*, explique François-Pierre Le Page, directeur général et cofondateur de Mobilegov.

Vingt-trois types de périphériques identifiés

Pour endiguer cette marée d'objets non sollicités, Mobilegov propose d'affecter à chaque équipement un identifiant unique, qu'il baptise Qualification Key Identifier (QKI). Cet « ADN numérique » est obtenu à partir des qualités intrinsèques du matériel : les paramètres de fabrication, les dimensions, la catégorie, etc.

Ces données issues des couches basses des équipements sont agrégées selon un procédé breveté en 2005, pour obtenir le QKI. Mobilegov peut reconnaître 23 types de périphériques différents, du stockage USB au moniteur en passant par la webcam, les cartes Bluetooth et les tablettes graphiques.

A partir de là, la solution DAPE permet de définir des règles de sécurité millimétrées. Basée sur un serveur et des agents logiciels, elle peut ne permettre sur certains postes que la connexion de certains périphériques, voire d'un seul en particulier. Le branchement d'un périphérique inconnu bloque automatiquement toute communication avec lui et l'administrateur est informé en temps réel. L'entreprise peut également définir des plages horaires pour certains types d'utilisation.

Le contrôle de l'intégrité des équipements en prime

Mais ce n'est pas tout. Comme le QKI est généré à partir des composants d'un matériel, il permet aussi d'assurer son intégrité physique. Si dans un PC un disque dur a été remplacé ou une barrette de mémoire subtilisée, l'ADN numérique ne correspond plus. Une notification est envoyée au service informatique.

Mais que faire si un périphérique autorisé est utilisé pour transférer des données sur un ordinateur externe, non géré par DAPE ? Là encore, Mobilegov propose une solution.

Les clés USB Device Linker du fournisseur embarquent la même technologie d'identification et permettent de limiter leur fonctionnement à certains ordinateurs pré-définis. Au moment de la connexion, la clé scanne le poste et vérifie simplement son « code génétique ». Le fournisseur envisage d'intégrer ce procédé dans d'autres équipements comme les disques durs.

Enfin, les tarifs de DAPE restent abordables. La solution coûte autour de 25 euros par poste protégé, plus 15 % sur le contrat global en service de maintenance.

FORUM : soyez le premier à vous exprimer !

L' « ADN numérique » des périphériques sécurise leurs connexions

Réagir

Le test des hébergeurs

Semaine du 12 au 18 décembre 2007

Internet FR, une remontée fulgurante

Après plusieurs semaines de chute, qui l'ont mené à l'avant-dernière place du classement, Internet FR est 1er cette semaine. Cette remontée spectaculaire est due au remplacement de But - qui plombait les résultats d'Internet Fr - par Veolia dans la liste des sites hébergés par Internet Fr et testé par IP Label...

moyenne du 18 11 au 18 12 2007

rang	hébergeurs	dispo. sites (sur 100)	performance d'accès aux sites (sur 100)	qualité globale (sur 100)	tendance
1	Internet FR	99.68	96.20	98.81	▲
2	Omis	99.54	96.47	98.77	▼
3	Pictime	99.91	95.18	98.73	▼
	Moyenne	98.88	93.04	97.28	

› 01net.com, en partenariat avec ip-label, mesure chaque semaine les performances des hébergeurs

> tous les classements des hébergeurs

Le test des opérateurs

Pour retrouver tout le test des opérateurs VoIP
› Cliquez ici

Agenda

A ne pas manquer !
› Salon Les jeudis-Emplois informatique & ingénierie le 10/01/2008
› Moteurs de recherche et intranet le 10/01/2008
› Conférence APE2008 du 22/01/2008 au 23/01/2008
› Progilog du 22/01/2008 au 24/01/2008

> tous les salons et séminaires


“ Sécurité du poste de travail ”
mobilegov®
Device Authenticator
PRO Edition
“Maîtriser l’usage des équipements amovibles dans l’entreprise
et prévenir les fuites des données.”
www.mobilegov.com

Garantir l'intégrité des postes clients : le défi des organisations

Le maintien de l'intégrité du Système d'Information est un ENJEU CAPITAL car une défaillance de celui-ci peut entraîner la perte de l'entreprise d'aujourd'hui.

La prolifération des ports sur ces postes de travail (USB, WIFI, BlueTooth, Firewire, HDMI, lecteurs de cartes multi formats, …) et les capacités de stockage grandissantes des périphériques amovibles (clefs USB, cartes, Disques externes, PDA, Smartphone, lecteurs MP3,…) sont un réel problème pour la sécurité des entreprises car ce sont autant de portes ouvertes non surveillées.

Malgré des investissements coûteux, la simple utilisation de périphériques amovibles fait tomber l'entière protection déployée sur vos réseaux et permet à tout un chacun "d'emprunter" des données sensibles ou d'introduire virus ou autres malwares potentiellement catastrophiques pour votre organisation.

Les solutions de protection traditionnelles, efficaces contre les attaques logicielles (Antivirus, Firewall, Anti-Spyware, Cryptage, etc.), ne sont plus suffisantes. Le vol d'informations confidentielles ou sensibles représente une réalité quotidienne (avec ou sans la complicité de l'utilisateur).

Le changement ou la modification de composants internes du poste de travail est également un danger, car ceci permet de passer au travers des solutions de sécurité mises en place par l'entreprise à son insu.

Les solutions traditionnelles ne sont plus suffisantes : 62% des entreprises qui sont infectées par un virus informatique avaient un antivirus installé.(source : Yankee Group, Forrester)

70% des attaques d'ordinateurs, des failles de sécurité ou du vol de données provient de l'intérieur des organisations. (Source : Yankee Group Security Leaders)

76% des entreprises reconnaissent qu'augmenter la sécurité de leurs systèmes les rend plus efficaces et leur donne un avantage compétitif sur leur marché.
(Etude Pen, Shoen & Berland Associates pour Business Software Alliance)

Les lois et régulations internationales telles que Sarbanes Oxley (contrôle des flux d'informations au sein des sociétés) ou l'HIPAA (vie privée des patients) imposent aux société de sécuriser les informations sensibles ainsi que leurs flux et transferts.

Autorisez l'utilisation des périphériques amovibles tout en maîtrisant les dangers.

Protéger votre entreprise et vos collaborateurs.

En complément de vos systèmes de protection actuels, indispensables, notre solution Device Authenticator PRO Edition permet de contrôler et de gérer les flux d'informations à travers les composants/périphériques internes et externes des entreprises et des organisations mais aussi d'auditer l'utilisation de ces périphériques.

- Sécurisez vos réseaux contre le VOL DE DONNEES et l'introduction de MALWARE au travers des ports de vos postes de travail (USB, bluetooth, Wifi, firewire, …)
- Contrôlez les CONNEXIONS INTERDITES et éviter le divertissement au travail (musique, vidéo, jeu) par des connexions d'iPods, de clés USB, de disques, etc…
- Garantissez la CONFORMITE AVEC LES LOIS ET REGULATIONS INTERNATIONALES (Sarbanes Oxley, HIPAA, …)
- Contrôlez les MODIFICATIONS MATERIELLES tels que les changements ou les modifications de composants internes (piratage des matériels, vol de pièces détachées, …)

La Solution

mobilegov
Device *Authenticator*
PRO Edition

Maîtriser l'usage des périphériques et profiter des gains de productivité qu'ils apportent.

Parce que l'ajout ou le changement d'un composant dans votre environnement informatique constitue une menace :

- **Protégez les postes clients contre le branchement de périphériques non autorisés.**
- **Définissez, gérez et appliquez facilement vos politiques de sécurité.**
- **Recevez sur votre serveur des notifications en temps réel des "mauvais usages".**
- **Etendez votre politique de sécurité à tous les périphériques amovibles avec ou sans fil.**

Authentifier, sécuriser, déployer…

Comment fonctionne Device Authenticator ?

Grâce à notre technologie, Device Authenticator PRO Edition permet l'identification forte et unique de tous les sous ensembles électroniques (clef, disques, PDA, smartphones, postes de travail, …) en utilisant des "protocoles de couches basses". Cette technologie unique est brevetée depuis 2005.

1. L'administrateur identifie les périphériques autorisés ou interdits, par famille ou individuellement.
2. Il spécifie les actions à entreprendre lors du branchement d'un périphérique non autorisé.
3. Ces règles sont déployées automatiquement depuis le serveur sur tous les postes qu'il souhaite protéger.
4. Les agents de Device Authenticator veillent régulièrement de manière transparente pour l'utilisateur, bloquant toute communication avec un périphérique non autorisé et informent l'administrateur en temps réel de toute infraction.
5. La solution permet de déterminer des plages horaires pour les politiques (horaires de bureau, salons, présentations clients, ...)
6. Les agents ont la connaissance des politiques, le Poste de Travail est protégé même lorsqu'il n'est plus sur le réseau de l'entreprise.
7. L'agent ne peut pas être désactivé par l'utilisateur.

Prenez l'avantage :

- Notre technologie repose sur l'utilisation de couches basses et non sur des services Windows.
- Gère les périphériques au niveau des paramètres de fabrication infalsifiables (n° de série, type et famille).
- Communications Agents/Serveur sécurisées et cryptées (certificats X509, cryptage RSA).
- Vérifie l'intégrité des composants internes d'une machine afin d'empêcher l'usurpation d'un poste de travail sur un réseau (création d'une identification unique de la machine).
- Détecte tout changement de configuration matérielle sur les postes clients et réagit selon la politique définie (désactivation du périphérique incriminé, alerte email, logoff…)
- Permet une gestion unitaire ou par classe.
- Fonction de Sauvegarde et de restauration incluse
- Permet l'association utilisateur/périphériques.
- Fonctionne sous Windows (XP Home et Pro, 2000, 2000 PRO, 2003)
- Recherche et tri avancé des alertes et logs.
- Fichiers de données cryptés
- Documentation en ligne intégrée
- Grande facilité d'installation et d'exploitation

EVOLUTIF

Puissant, fiable, intuitif

- Seul Device Authenticator PRO Edition permet de sécuriser les équipements mobiles tels que PDAs ou smartphones en évitant de les utiliser comme passerelle.
- L'architecture client/serveur rend Device Authenticator évolutif quelque soit le nombre de pc dans l'entreprise.
- Fonctionne sous Windows (Linux, Mac, autres sur demande).
- Echanges sécurisés (certificats X509, cryptage MD5, RSA, SHA1)
- Disponible en Anglais et Français.
- Impacte les performances de façon minime.
- Protection active: le poste client reste protégé même s'il n'est pas connecté au réseau.

TECHNOLOGIE PORTABLE

Grâce à la technologie unique d'identification matérielle de Mobilegov, Device Authenticator n'est pas dépendant du système d'exploitation.
Notre solution peut être adaptée à une multitude d'environnements et peut supporter un réseau hétérogène.

CLASSES DE PERIPHERIQUES IDENTIFIES

1. Stockage USB - Clé USB, Disque dur externe USB,
2. Stockage IEEE 1394 - Disque dur externe FireWire,
3. Stockage SCSI - Disque dur SCSI,
4. Stockage IDE - Disque dur IDES,
5. Lecteur de disquettes - Lecteur de disquettes 3.5/5.25,
6. Disque Optique - Lecteur CDROM/DVD, Graveurs,
7. Port Parallèle,
8. Port Série - COM,
9. Infrarouge - Port IrDA,
10. PCMCIA,
11. Periphérique Biométrique - Lecteur de carte à puce, lecteur d'empreintes.
12. Périphérique d'imagerie USB - Appareil Photo, Scanner,
13. Webcam,
14. Périphérique TV USB - Périphérique TV USB à base de composants 28xx.
15. Son - Carte Son, Microphone,
16. Imprimante,
17. Carte Réseau - Carte Ethernet, Carte WIFI,
18. Modem RNDIS,
19. Bluetooth - Carte Bluetooth,
20. PDA - PDA, Smartphone,
21. Clavier,
22. Pointage - Souris, Tablette Graphique,
23. Moniteur.

mobilegov
Device *Authenticator*
PRO Edition

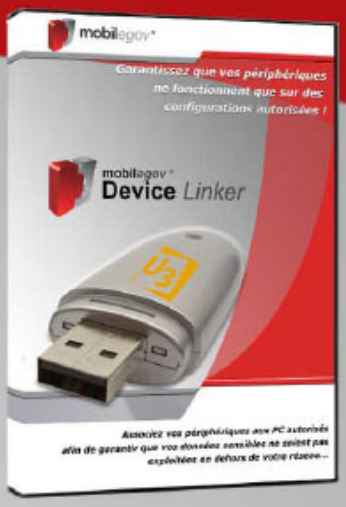
Mobilegov France
2000, route des Lucioles - Les Algorithmes
06901 Sophia Antipolis
France

Tel : +33 492 944 894
Fax : +33 492 944 895

Mobilegov UK
200 Brook Drive - Green Park
Reading RG2 6UB
United Kingdom

Tel : +44 118 949 7000
Fax : +44 118 949 7001

mobilegov
Device Linker



Pour que vos périphériques de stockage de données ne fonctionnent que sur vos machines !

La prolifération de périphériques de stockage de grande capacité tels que Clés USB, iPod®s, PDAs, Graveurs, Caméras et autres gadgets avec ou sans fil, introduit une nouvelle menace de sécurité dans les entreprises et les administrations publiques où des données sensibles peuvent être dérobées.

Device Authenticator® vous protège contre ce risque.

D'autre part, vous stockez des données sensibles sur vos périphériques amovibles.

Etes-vous protégé en cas de perte ou de vol du périphérique ?

Les protections à base de mot de passe ou de biométrie sont sans effet face à des personnels consentants ou menacés.

Device Linker® vous protège contre :

▶▶ Le vol de données informatiques, en rendant vos données illisibles en dehors de votre environnement (vos machines, votre réseau).

▶▶ Le vol de périphériques de stockage, en les rendant inutilisables.

Protégez-vous contre :

L'UTILISATION DE VOS PERIPHERIQUES USB U3 SUR DES PCs NON AUTORISES

La technologie Linker® rend vos périphériques USB U3 inutilisables en dehors de votre environnement (réseau, pool de machines).

LA PERTE OU LE VOL DE VOS CLES USB U3

Tant que la clé USB ne reconnaît pas la configuration sur laquelle elle est connectée, elle reste inutilisable et l'accès aux données qu'elle contient est impossible !

Device Linker® ne nécessite aucune modification de votre environnement informatique. La protection s'applique à tous les périphériques U3 existants.

Une interface d'administration simple vous permet de configurer vos périphériques et les hôtes sur lesquels ils fonctionneront.

U3 smart

www.devicelinker.com

mobilegov
Device Linker

Device Linker® intègre la technologie de sécurité brevetée de MobileGov. U3 fournit des clés USB sécurisées ayant deux partitions : une partition CDROM (lecture seule) lançant un logiciel dès l'insertion de la clé et une partition privée, protégée par un mot de passe (sans ce mot de passe, cette partition est inaccessible en lecture et en écriture).

Device Linker® permet à une clé U3 d'être utilisée sur un groupe de machines préalablement autorisé et d'être inutilisable sur les autres machines.

Device Linker® régit l'accès à la partition protégée (contenant vos données).

Fonctionnement schématisé :

Comment fonctionne Device Linker®

1. Au cours d'une première étape de configuration, le périphérique est connecté à n'importe quel PC du Réseau afin de définir l'environnement sur lequel il pourra être utilisé : ce PC, un groupe de PC, le LAN sur lequel le PC est lui-même connecté.

2. Il faut ensuite définir les mesures à prendre si le périphérique est connecté à un environnement imprévu : rendre le périphérique illisible, transmettre discrètement des informations sur l'environnement, détruire les données ou demander une autorisation d'usage temporaire.

Principales fonctionnalités :

▶▶ Définition dynamique des environnements : sélection des paramètres d'identification d'une machine hôte à partir d'une liste préétablie (CPU/ OS/ cartes mère/ etc.).

▶▶ Gestion des machines hôtes : enregistrement direct sur une machine non identifiée et gestion des listes de machines autorisées.

▶▶ Enregistrement des modifications sur la clé et gestion transparente et sécurisée (mot de passe généré inconnu de l'utilisateur) d'une partition chiffrée et cachée.

▶▶ Options de backup et de restauration des clés

▶▶ Edition Personnelle (grand public) et Entreprise (administration de groupes de clés Linker, des remontées d'alertes, …).

▶▶ Peut s'utiliser conjointement avec Device Authenticator® (voir http://deviceauthenticator.com), les clés Device Linker pouvant ainsi être intégrés à la logique de sécurité réseau.

Principaux matériels compatibles :

Certifié U3, Device Linker® reconnaît les matériels informatiques USB U3

mobilegov
2000, Route des Lucioles
Les Algorithmes
06901 Sophia Antipolis, France
Tel: +33.492.944.894
Fax: +33.492.944.895
mail: info@mobilegov.com
Sandgate House 102 Quayside
Newcastle upon Tyne NE1 3DX
United Kingdom