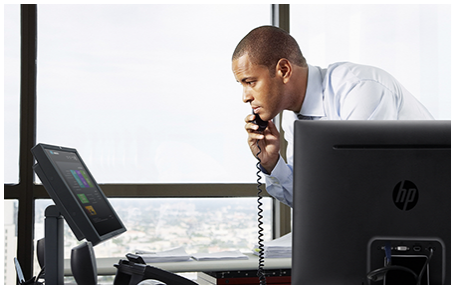
Protection contre la Fuite des données, priorité pour les entreprises ?

	Protection contre la Fuite des données, priorité pour les entreprises ?

Prévention des pertes de données des collaborateurs mobiles. Quand la mobilité oblige à la Data Loss Prevention.



La mobilité est à la fois un besoin et un défi pour les entreprises qui se battent pour créer une force de travail réellement fluide et entièrement digitale. Aujourd'hui, presque tous les collaborateurs travaillent avec un ou plusieurs périphériques mobiles contenant des informations d'entreprise, qu'il s'agisse d'un téléphone mobile, d'un ordinateur portable ou d'une tablette. L'un des premiers défis qui en découlent pour la direction informatique tient au fait que l'accès à distance aux données et aux e-mails se fait, par nature, « hors » du périmètre de l'entreprise, et qu'il est par conséquent très difficile de s'en protéger. La multitude des périphériques utilisés, en elle-même, complique la surveillance et le suivi des données d'entreprise consultées, partagées ou utilisées.

Data Loss Prevention : se concentrer sur les données

L'une des approches, choisie dans certaines entreprises, consiste à intégrer ces périphériques à une stratégie d'environnement de travail en BYOD. Les utilisateurs peuvent choisir le périphérique, le système d'exploitation et la version de leur choix, puisqu'il s'agit de leur propre périphérique. Malheureusement, cette approche peut en réalité créer des problèmes supplémentaires de sécurité et de DLP (prévention des pertes de données). En effet, de nombreux utilisateurs n'apprécient pas (voire interdisent) que leur employeur gère et/ou contrôle leur périphérique, pire encore, d'y installer des logiciels professionnels comme les programmes d'antivirus et de **VPN**.

Par conséquent, pour réussir, la stratégie de protection des données doit se concentrer sur la sécurisation des données uniquement, quel que soit le périphérique ou le mode d'utilisation. Dans un environnement d'entreprise, une grande majorité des données sensibles transitent dans les e-mails et leurs pièces jointes. Ainsi, une stratégie de protection des données réussie doit chercher à gérer et contrôler la passerelle par laquelle transitent les données, à savoir, ici, le compte d'e-mail d'entreprise.

Autre option : implémenter une suite d'outils de gestion de la sécurité mobile, ce qui permet de placer des mécanismes de sécurité sur la passerelle d'e-mail, et d'autoriser la création de règles de sécurité pour surveiller et contrôler la façon dont les informations d'entreprise sont traitées sur chaque périphérique.

Data Loss Prevention : Stratégie DLP tridimensionnelle

Une stratégie « DLP tridimensionnelle », surveille et contrôle le contenu transféré via un périphérique sur la base de critères précis. Par exemple, on peut limiter l'accès au contenu ou aux fichiers depuis le compte e-mail d'entreprise en fonction du pays, puisque les utilisateurs qui voyagent avec leur périphérique sont susceptibles d'accéder aux données et aux systèmes sur des réseaux Wi-Fi non sécurisés. Il est également possible de contrôler le contenu sur la base des mots clés qui figurent dans les e-mails (comme des numéros de sécurité sociale ou des numéros de contrat), afin d'interdire les pièces jointes ou le contenu incluant ce type d'information sur les périphériques mobiles. Comme les pièces jointes d'e-mail contiennent la majorité des informations sensibles transmises d'un périphérique à un autre, ce point est crucial lorsqu'il s'agit de protéger l'utilisation des périphériques dans l'environnement de travail. La troisième dimension est la surveillance du contexte, qui permet d'identifier et d'interdire le contenu pour des expéditeurs/destinataires spécifiques.

Ce type de considération permet de limiter les risques liés aux pertes de données et aux problèmes de sécurité pour cette partie des activités professionnelles Bien que cette approche ne suffise pas à contrôler et à sécuriser entièrement les banques de données d'une entreprise, la sécurité mobile va jouer un rôle de plus en plus vital pour la réussite des stratégies complètes de protection des données, au fur et à mesure que davantage de périphériques s'intègrent à nos habitudes de travail. (Par Eran Livne, Product Manager LANDESK)

Article original de Damien Bancal

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Data Loss Prevention – Data Security BreachData Security Breach