Les dix bonnes pratiques de l'ENISA en matière de sensibilisation à la sécurité

Juillet 09

enisa
European Network and Information Security Agency

Au sujet de l'ENISA

L'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) est une agence européenne qui a été créée pour servir le fonctionnement du marché intérieur. L'ENISA est un centre d'excellence en matière de sécurité des réseaux et d'information pour les États membres et les institutions de l'Union européenne. Elle prodigue conseils et recommandations et agit comme une centrale d'informations en matière de bonnes pratiques. En outre, elle facilite les contacts entre les institutions européennes, les États membres, les entreprises privées et les acteurs de l'industrie.

Coordonnées

Pour toute information générale ou concernant la sensibilisation à la sécurité de l'information, veuillez nous contacter à l'adresse électronique suivante:

Courriel: Isabella Santa, Responsable Sensibilisation — awareness@enisa.europa.eu

Internet: http://www.enisa.europa.eu

Les dix bonnes pratiques de l'ENISA en matière de sensibilisation à la sécurité

Juillet 2009

Sommaire

Synthèse

La présente brochure aborde certains points essentiels de la sensibilisation aux technologies de l'information et de la communication (TIC) dans les entreprises. Elle présente des bonnes pratiques en matière de sécurité avec pour objectif d'attirer l'attention des employés sur la sécurité de l'information, de leur permettre de reconnaître les problèmes de sécurité informatique et d'y répondre de manière adéquate.

Ces bonnes pratiques peuvent être utilisées comme un guide sur les principales mesures à prendre dans le cadre de la sensibilisation à la sécurité de l'information. L'ENISA a réalisé cette brochure pour sensibiliser les employés aux risques qui pèsent sur la sécurité de l'information et leur rappeler les règles d'or dans ce domaine. La brochure peut être utilisée dans le cadre de tout programme sur la sécurité de l'information, de toute activité de sensibilisation à ce thème ainsi que sur le site web des entreprises.

Les dix bonnes pratiques de l'ENISA en matière de sécurité font partie de l'ensemble des outils développés pendant la campagne européenne de sensibilisation à la sécurité de l'information lancée par l'Agence.

Les dix bonnes pratiques de l'ENISA en matière de sensibilisation à la sécurité

Suite à de récents incidents de grande ampleur portant sur des informations confidentielles, les grandes organisations privées et publiques ont compris qu'elles devaient mettre en place des politiques et développer des moyens technologiques pour garantir la sécurité de leurs informations internes sensibles. Ces mesures de contrôle doivent permettre de sécuriser les informations présentes sur leur réseau et de gérer les données qui entrent et sortent de l'entreprise. Si ces politiques et moyens technologiques constituent sans aucun doute un aspect essentiel de tout programme de protection de l'information, ils ne peuvent, en pratique, garantir à eux seuls un niveau suffisant de sécurité de l'information.

Le meilleur moyen de garantir cette sécurité est de sensibiliser les personnes concernées aux risques et aux outils de protection existants. Les employés représentent le périmètre invariable de tout réseau d'entreprise; dès lors, leur comportement devient un élément incontournable de l'ensemble du système de sécurité. Pour se protéger, les organisations doivent commencer par s'assurer que leurs employés comprennent leur rôle et leurs responsabilités dans la sauvegarde des données sensibles et des ressources internes, et aident l'entreprise à garantir la sécurité des ordinateurs et du réseau informatique.

À cette fin, l'ENISA déploie ses efforts pour orienter les employés vers une meilleure approche de la sécurité de l'information et changer l'état d'esprit de la composante humaine des entreprises, afin d'obtenir une plus grande implication de chacun en faveur de la sécurité de l'information.

L'Agence a donc réalisé cette brochure qui récapitule dix bonnes pratiques en matière de sécurité. Ces bonnes pratiques constituent un outil très efficace pour sensibiliser les employés aux risques qui pèsent sur la sécurité de l'information et leur rappeler les règles d'or à respecter dans ce domaine.

Le présent document a été réalisé à l'intention de toutes les organisations chargées de lancer des initiatives visant à aider les employés à apprendre comment ils peuvent protéger les informations et le capital de leur entreprise de manière proactive.

1. Utilisation d'un mot de passe

Votre mot de passe est l'équivalent de la serrure et de la clé de votre maison, sur l'internet. Les mots de passe constituent l'un des principaux moyens de défense; acquérir de bons réflexes dans ce domaine vous aidera à mieux protéger vos informations personnelles sensibles et vos données d'identification.

Utilisez un mot de passe sûr

- ✓ Le mot de passe de votre ordinateur est la clé pour accéder à toutes les informations — professionnelles et personnelles — que vous avez stockées sur votre ordinateur et sur vos comptes en ligne. Utilisez un mot de passe sûr pour protéger vos données: il doit comporter au moins huit caractères et associer des lettres (majuscules et minuscules), des nombres et des symboles. Plus votre mot de passe contient de caractères différents, plus il est difficile à deviner. N'utilisez pas d'informations personnelles telles que votre nom, celui de vos enfants, leur date d'anniversaire, etc. que quelqu'un pourrait connaître ou obtenir facilement, et essayez d'éviter les mots communs: certains hackers utilisent des programmes qui testent chaque mot du dictionnaire.

Modifiez votre mot de passe régulièrement

- ✓ Si vous pensez que votre système a été atteint, modifiez immédiatement vos mots de passe.

Tenez votre mot de passe secret

- ✓ Votre mot de passe est unique et ne doit être divulgué à personne.
- ✓ Lorsque possible, essayez de mettre en place une stratégie vous permettant de mémoriser vos différents mots de passe.
- ✓ Si vous écrivez vos mots de passe quelque part, soyez prudent quant au lieu où vous stockez cette information. Ne laissez une trace écrite dans aucun endroit où vous ne laisseriez pas les informations que vos mots de passe sont sensés protéger.

Utilisez des mots de passe différents

- ✓ Utilisez un mot de passe différent pour chaque compte en ligne auquel vous avez accès (ou au moins plusieurs mots de passe). Si vous utilisez le même mot de passe pour plusieurs comptes, un «agresseur» ayant réussi à accéder à l'un de vos comptes, pourra faire de même pour tous les autres.

2. Protégez votre ordinateur

- ✓ Verrouillez votre ordinateur fixe lorsque vous quittez votre bureau pour assister à une réunion, faire une pause et/ou prendre votre déjeuner.
- ✓ N'autorisez pas les autres personnes à connecter leur clé USB à votre ordinateur, surtout s'il s'agit d'une clé personnelle non sécurisée.
- ✓ N'installez pas, et n'utilisez pas de logiciel illégal et/ou non autorisé car cela peut compromettre la sécurité de vos données et constituer une violation de la loi. Des programmes extérieurs inconnus peuvent identifier les failles de sécurité du réseau de votre organisation et s'y introduire.
- ✓ Ne connectez aucun disque ou lecteur de musique personnel ni aucune clé USB à votre ordinateur.
- ✓ Ne connectez pas votre ordinateur portable personnel au réseau de votre organisation car il peut être infecté par un virus ou atteint par un programme malveillant.

3. Utilisez la messagerie électronique et l'internet avec précaution

- ✓ N'ouvrez pas les courriels non identifiés ni leurs pièces jointes.
- ✓ Ne cliquez pas sur les liens hypertexte contenus dans les courriels suspects.
- ✓ Transférez vos courriels si nécessaire mais pensez à en supprimer l'historique au préalable.
- ✓ Envoyez des documents au format PDF pour être sûr(e) qu'ils ne pourront pas être facilement modifiés.
- ✓ Toute information confidentielle doit être cryptée lorsqu'elle est communiquée par messagerie électronique.
- ✓ Surfez sur l'internet avec précaution.

- ✓ Ne communiquez pas d'information sur votre organisation et vos fonctions sur des sites de réseau social.
- ✓ Évitez de contribuer à des blogs sur lesquels votre avis et vos opinions pourraient être considérés comme reflétant ceux de votre organisation.
- ✓ Ne téléchargez aucun document ou matériel provenant de parties auxquelles vous ne faites pas confiance.
- ✓ Ne cherchez pas à accéder à du matériel illégal ou destructeur, ni à le télécharger, le stocker ou l'envoyer.
- ✓ N'oubliez pas que lorsque vous surfez sur l'internet depuis votre poste de travail, celui-ci peut être identifié.

4. Utilisation d'appareils portables de l'entreprise: ordinateurs portables, clés USB, téléphones portables et BlackBerrys

Ordinateurs portables

- ✓ N'installez ou n'utilisez pas de logiciel illégal et/ou non autorisé car ce faisant, vous compromettez la sécurité de vos données et enfreignez la loi.
- ✓ Éteignez les connections sans fil lorsque vous n'en avez pas besoin.
- ✓ Connectez régulièrement votre ordinateur portable au réseau de votre organisation afin de mettre à jour les contrôles de sécurité.
- ✓ Faites une copie des informations stockées sur votre ordinateur portable.
- ✓ Verrouillez votre ordinateur portable lorsque vous quittez votre bureau pour assister à une réunion, faire une pause ou prendre votre déjeuner.
- ✓ N'autorisez pas d'autres personnes à connecter leur clé USB à votre ordinateur, surtout s'il s'agit d'une clé personnelle non sécurisée.
- ✓ Ne laissez pas votre ordinateur portable sans surveillance.
- ✓ Ne laissez pas votre ordinateur portable dans votre voiture à la vue de tous.

Clés USB

- ✓ Utilisez une clé USB cryptée.
- ✓ Limitez le nombre de données professionnelles stockées sur votre clé USB, surtout s'il s'agit d'une clé personnelle non sécurisée.
- ✓ Attachez votre clé USB à un porte-clé ou à un cordon afin d'éviter de la perdre: en effet, du fait de leur taille réduite, les clés USB se perdent ou se volent facilement. En outre, plus la capacité de stockage est élevée, plus le nombre de données potentiellement menacées est important. Une clé USB est généralement placée dans un sac, un sac à dos, une malette d'ordinateur portable, une veste, la poche d'un pantalon, ou laissée sans surveillance sur le bureau. Récemment, les cas de clés USB perdues, égarées, empruntées sans permission ou volées ont augmenté.
- ✓ Invitez les utilisateurs à mettre leur clé USB en mode «lecture seule» en utilisant le petit interrupteur réservé à cet effet; cela permettra d'éviter la transmission de virus. Certaines clés USB comprennent une commande qui permet un fonctionnement en mode «lecture seule»: ainsi, l'ordinateur hôte ne pourra écrire ou modifier des données sur la clé.
- ✓ Contrôlez votre clé USB après avoir copié des fichiers à partir d'un ordinateur non sécurisé ou non autorisé, pour détecter toute transmission de virus.
- ✓ Avant d'insérer votre clé USB dans l'ordinateur d'une autre personne, effacez tous les fichiers dont vous n'avez pas besoin dans le cadre de cette action.
- ✓ Sauvegardez vos données pour pouvoir retrouver les informations stockées sur vos clés USB.

Téléphones portables et BlackBerrys

- ✓ Débranchez les connections sans fil (c'est-à-dire Bluetooth et WLAN) lorsque vous ne les utilisez pas. La technologie Bluetooth permet à des dispositifs électroniques de communiquer entre eux via une connexion radio à basse fréquence. Certains appareils portables Bluetooth sont sujet à des bugs logiciels, ce qui conduit aux pratiques du *Bluejacking* et du *Bluesnarfing* (intrusion Bluetooth et vol de données Bluetooth).
  Avec le «Bluejacking», une personne vous envoie un texte anonyme en créant un nouveau message, puis l'envoie à un autre téléphone portable sur lequel la technologie Bluetooth est activée. Le «Bluejacking» peut être utilisé pour envoyer des messages indésirables.
  Le «Bluesnarfing» est utilisé pour copier des informations personnelles, comme la liste des contacts, du téléphone portable de quelqu'un d'autre.
- ✓ Ne laissez pas votre téléphone portable ou votre BlackBerry sans surveillance, cela pourrait conduire à une perte de données.

5. Manipulez les informations avec précaution

- ✓ Répertoriez chaque document selon un code de classification approprié.
- ✓ Protégez tout contenu sensible avec un mot de passe afin que personne ne puisse le modifier ou l'effacer.
- ✓ Appliquez la politique du bureau bien rangé: ne laissez pas des données sensibles autour de votre poste de travail. Rangez soigneusement vos documents.
- ✓ Ne laissez pas d'information sensible dans des salles de conférence ou de réunion partagées, ceci évitera qu'une personne utilisant la salle après vous n'en prenne connaissance.
- ✓ Impression sécurisée: imprimez, copiez et scannez des informations seulement si cela est nécessaire. N'oubliez pas de récupérer vos impressions dans le tiroir de sortie de l'imprimante.
- ✓ Détruisez toujours les documents qui contiennent des informations sensibles et/ou classées confidentielles.
- ✓ Ne stockez aucune information sur votre disque local.
- ✓ Avant de communiquer une quelconque information sensible à un tier avec qui vous travaillez, assurez-vous qu'il a bien signé une clause de confidentialité.

6. Visiteurs

- ✓ Tous les visiteurs doivent être enregistrés à leur arrivée et à leur départ.
- ✓ Tous les visiteurs doivent se voir remettre un badge d'identification à porter pendant toute la durée de leur visite dans les locaux de l'entreprise.
- ✓ Accompagnez les visiteurs dans vos locaux professionnels à tout moment. Il n'est pas prudent de laisser les visiteurs s'y promener.

7. Signalez toute perte et/ou détérioration de vos appareils portables d'entreprise, et tout incident

- ✓ Signalez au service informatique de votre organisation toute perte et/ou

détérioration de vos appareils portables professionnels (tels que téléphone portable, PDA ou clé USB).

- ✓ Signalez au service informatique de votre organisation tout appareil portable professionnel trouvé.
- ✓ Signalez tout manquement aux règles de sécurité et/ou incident, même si vous n'en avez pas la certitude.
- ✓ Signalez toute activité suspecte sur votre poste de travail et tout mauvais fonctionnement d'une application dont le service informatique ne vous aura pas averti au préalable.

8. Protégez les informations en-dehors de votre entreprise

- ✓ Lorsque vous êtes hors de votre entreprise, assurez-vous à tout moment que vos informations et votre équipement sont en sécurité afin de prévenir un vol ou une perte. Lorsque vous êtes dans des lieux publics en particulier, manipulez les informations avec précaution.
- ✓ N'oubliez pas qu'une personne peut entendre votre conversation. Ne portez pas les informations confidentielles de votre société sur la place publique.
- ✓ Lorsque vous voyagez ou lorsque vous travaillez à distance, méfiez-vous des personnes indiscrètes (qui suivent vos conversations par dessus votre épaule).

9. Respectez la politique et les procédures de sécurité de l'entreprise

- ✓ Respectez la politique et les procédures de sécurité mises en place par l'entreprise.
- ✓ Veillez à conserver la confidentialité, l'intégrité et la disponibilité des données.
- ✓ Respectez les dispositions juridiques telles que les droits d'auteur, la propriété intellectuelle, la protection de la vie privée et les licences logicielles.
- ✓ Si vous vous apercevez que certains collègues enfreignent la politique ou les procédures de sécurité de l'entreprise, signalez-le immédiatement.

10. Donnez votre avis pour améliorer les solutions et la politique de sécurité en vigueur

- ✓ Donnez votre avis pour améliorer les solutions et la politique de sécurité en vigueur .
- ✓ Suggérez l'achat de tout logiciel complémentaire nécessaire à l'accomplissement de vos tâches.
- ✓ Posez des questions ou faites des suggestions visant à améliorer les solutions et les mesures de sécurité.

Conclusions

Les informations doivent être protégées contre toute consultation non autorisée et les employés doivent comprendre leur rôle et leurs responsabilités dans la sauvegarde des données sensibles et la protection du capital de leur entreprise.

Les employés doivent savoir ce qu'ils peuvent et ce qu'ils ne peuvent pas emporter chez eux (ordinateurs portables d'entreprise, etc.), ce qu'ils peuvent et ne peuvent pas faire avec les documents de la société, et les mesures à prendre, le cas échéant, pour effectuer des copies de sauvegarde et utiliser les moyens technologiques de sécurité disponibles.

L'ENISA s'engage donc à guider les employés vers davantage de sécurité de l'information, à modifier l'état d'esprit de cette composante humaine de l'entreprise afin de parvenir à une plus grande sensibilisation individuelle à la sécurité de l'information.

En gardant à l'esprit ces bonnes pratiques en matière de sécurité, les employés seront plus attentifs à la sécurité de l'information, ce qui leur permettra de reconnaître les risques de sécurité informatique les plus courants et d'y répondre de manière adéquate.

Références

ENISA, *Clés USB: priorité à la sécurité*, Juin 2008:
http://www.enisa.europa.eu/act/ar/deliverables/2008/secure-usb-flash-drives-fr

ENISA, *Impression sécurisée*, Avril 2008:
http://www.enisa.europa.eu/act/ar/deliverables/2008/secure-printing-fr

Les dix bonnes pratiques de l'ENISA en matière de sensibilisation à la sécurité

ISBN-13: 978-92-9204-044-4

Doi: 10.2824/18080

Catalogue number: TP-80-10-258-FR-N

TP-80-10-258-FR-N

ISBN-13 978-92-9204-044-4

PO Box 1309, 71001 Heraklion, Greece, Tel: +30 2810 391 280
www.enisa.europa.eu