

Les bonnes pratiques contre les Cyberattaques | Denis JACOPINI

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer

 LE NET EXPERT AUDITS & EXPERTISES	 EXPERTISES DE SYSTÈMES DE VOTES ÉLECTRONIQUES LENETEXPERT .fr	 RGPD CYBER LENET EXPERT MISES EN CONFORMITÉ	 SPY DETECTION Services de détection de logiciels espions	 LE NET EXPERT FORMATIONS	 LE NET EXPERT ARNAQUES & PIRATAGES
<input checked="" type="checkbox"/>	Les bonnes pratiques contre les Cyberattaques				

Pour se prémunir des cyberattaques, la meilleure solution consiste à mettre en place quelques bonnes pratiques de base.

Encourager une gestion rigoureuse des mots de passe

Mettez en place des outils qui forcent les utilisateurs à choisir des mots de passe forts. Ceux-ci comprennent au moins huit caractères, des majuscules et des minuscules, des chiffres et des symboles du clavier (!, @, \$, etc.), mais aucun mot entier. Ils doivent aussi être changés régulièrement, même si ça cause de la grogne.

Sensibiliser les employés

Souvent considérés comme la porte d'entrée des cybercriminels, les employés doivent être formés, par exemple au moyen de modules d'apprentissage vidéo, sur les risques d'attaques possibles et les différentes formes qu'elles peuvent prendre.

Effectuer régulièrement des tests

Une façon de vérifier si les campagnes de sensibilisation auprès des employés fonctionnent consiste à les tester en simulant, par exemple, l'envoi d'un courriel frauduleux. N'oubliez pas de l'envoyer aussi – et même surtout – à ceux qui occupent des postes stratégiques.

Limiter l'accès à l'information confidentielle

Ne donnez accès aux renseignements confidentiels qu'à ceux qui en ont réellement besoin dans l'entreprise.

Contrôler les processus de sécurité

Rien ne sert d'avoir des systèmes informatiques à la fine pointe si on ne les teste pas régulièrement. Il vaut mieux impartir la tâche à des experts si on ne possède pas les ressources nécessaires à l'interne. Les fournisseurs de solutions infonuagiques disposent d'une infrastructure de sécurité informatique qui peut bien souvent dépasser celle des entreprises.

Installer les mises à jour logicielles rapidement

Beaucoup d'attaques exploitent des vulnérabilités connues depuis plusieurs mois par les fournisseurs d'antivirus, qui d'ailleurs offrent déjà des correctifs pour les contrer. Prévoyez l'installation des mises à jour dans un délai optimal de 48 heures, ou d'au plus une semaine.

Nous vous conseillons les ouvrages suivants :

Guide de la survie de l'Internaute



Dans ce guide pratique, vous trouverez des conseils et un vrai savoir faire dans le domaine de l'identité Internet et de la recherche par recouplement d'informations.

Anti-Virus-Pack PC Sécurité

☒
Moyen pour détecter et chasser les Virus et autres Spyware, ou Protéger Votre PC avant qu'il ne soit TROP tard ...

[block id="24761" title="Pied de page HAUT"]

Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :

Les 10 conseils pour ne pas se faire «hacker» pendant l'été

Les meilleurs conseils pour choisir vos mots de passe

Victime d'un piratage informatique, quelles sont les bonnes pratiques ?

Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?

Attaques informatiques : comment les repérer ?

[block id="24760" title="Pied de page BAS"]

Source :
<http://www.lesaffaires.com/dossier/gestion-des-risques/cyberattaques-toutes-les-bonnes-pratiques/579165>