Édu_Num Économie et gestion
Hors-série n°3
Mai 2017 - Cybersécurité dans les organisations

Sommaire

1. COMPRENDRE LA CYBERSÉCURITÉ DANS LES ORGANISATIONS

1.1 La France et la cybersécurité

Après avoir défini la cybersécurité, cet article, publié par le Ministère des Affaires étrangères et du Développement international, présente notamment les orientations stratégiques prises ces dernières années au plus haut niveau de l'État français.

Lire l'article

1.2 Cybersécurité 2017 : les dix nouveaux commandements

Les Échos Business proposent dix conseils pour contrer les risques liés à des cyberattaques menées à l'encontre des organisations.

Lire l'article

1.3 Baromètre Cybersécurité 2017 : où en est l'industrie française ?

Cette infographie présente une étude réalisée auprès de dirigeants du CAC 40 et de 200 cadres supérieurs sur le sujet des cyber-risques auxquels est soumise l'industrie française aujourd'hui.

Voir l'infographie

1.4 Et si demain vous faisiez attention à votre cybersécurité ?

La chronique de Catherine Boulay sur France Inter revient sur le forum de la cybersécurité qui s'est tenu au mois de janvier 2017 à Lille. Parmi les sujets abordés, il y a été question de cette menace qui monte : le "ransomware". Le principe est très simple : un pirate prend en otage les données d'un ordinateur. Pour les récupérer, il demande au propriétaire une rançon.

Écouter l'émission

1.5 Mesurez-vous aux hackers de la Hack Academy !

Le CIGREF est une association loi 1901 dont la mission est de "développer la capacité des grandes entreprises à intégrer et maîtriser le numérique". Le CIGREF a choisi l'humour et un ton décalé pour une campagne destinée à sensibiliser le grand public aux risques sur internet, à travers 4 films abordant 4 risques auxquels chacun peut être exposé : vol de mots de passe, paiements faussement sécurisés, logiciels malveillants et hameçonnage (phishing).

Voir les vidéos

2. LA CYBERSÉCURITÉ DANS LES ORGANISATIONS EN PRATIQUE

2.1 Une cyberattaque historique frappe le monde

200 000 victimes dans 150 pays : c'est le premier bilan de la cyberattaque qui frappe le monde depuis vendredi 12 mai 2017. Un message exige une somme d'argent pour déverrouiller le système des ordinateurs infectés. La propagation semble enrayée grâce à un Britannique de 22 ans qui est parvenu à bloquer la diffusion du virus.

Voir la vidéo

2.2 Cyberattaque mondiale : Renault-Nissan dans l'œil du cyclone

Le constructeur automobile a dû mettre une partie de sa production à l'arrêt après que plusieurs sites aient été infectés par le logiciel rançonneur WannaCry.

Voir l'article

2.3 Le Day-Click 2016 : conférence cybersécurité

Le Syntec Numérique à travers sa marque Talents du Numérique a organisé le 18 octobre 2016, la première édition du Day-Click, événement regroupant en une seule et même journée jeunes générations, startups, investisseurs, écoles et entreprises du secteur numérique.Nicolas Arpagian, Directeur scientifique du Cycle "Sécurité Numérique" de l'Institut National des Hautes Études de la Sécurité et de la Justice (INHESJ) et maître de conférences à l'École Nationale Supérieure de la Police

(ENSP) a donné une conférence sur le thème de la cybersécurité : un secteur en forte croissance.
Voir la vidéo

2.4 Les grands enjeux cyber 2016 : la face cachée de la cybersécurité

Au travers de cas et d'une enquête, le groupe Deloitte met en avant les aspects visibles et moins visibles de la gestion des risques cyber. Il revient sur trois enjeux incontournables en matière de sécurité de l'information : la transformation digitale, la protection des données et la réglementation, l'authentification.

Lire l'article

2.5 Guide des bonnes pratiques de l'informatique dans les PME

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) et la Confédération générale des petites et moyennes entreprises (CGPME) présentent douze règles essentielles pour la sécurité des systèmes d'information des petites et moyennes entreprises. L'usage de l'informatique s'est généralisé dans les TPE/PME. Corollaire de cette évolution, de nouveaux risques ont émergé : vols de données, escroqueries financières, sabotage des sites de e-commerce. Les entreprises doivent se doter d'une politique de sécurisation des systèmes d'information inhérente à l'usage des nouvelles technologies.

Voir le guide

2.6 Calculer la "force" d'un mot de passe

Par abus de langage, on parle souvent de "force" d'un mot de passe pour désigner sa capacité à résister à une énumération de tous les mots de passe possibles. L'Agence nationale de la sécurité des systèmes d'information (ANSSI) propose un calculateur qui estime la "force" d'un mot de passe par comparaison avec les techniques cryptographiques.

Accéder au calculateur

2.7 Les entreprises peinent à appliquer leur stratégie cybersécurité

D'après une étude mondiale commanditée par Intel, 90% des entreprises ont défini une stratégie de cybersécurité mais ont des difficultés à la mettre en œuvre. De plus, le chevauchement des technologies de sécurité entraine également des risques de vulnérabilités.

Lire l'article

2.8 La cybersécurité, nouveau talon d'Achille du secteur aéronautique ?

Selon le cabinet Deloitte, tous les indicateurs économiques sont au vert pour le secteur aéronautique. Mais, un nouveau risque majeur est à craindre : des cyberattaques qui pourraient menacer la sécurité des vols.

Lire l'article

2.9 Yahoo! : comment un demi-milliard de comptes ont été piratés

Au mois de mars 2017, les autorités américaines ont accusé quatre personnes, dont deux membres des services de renseignement russes FSB, d'être responsables d'une cyberattaque massive contre le groupe américain Yahoo ! en 2014.
Cette cyberattaque aurait permis aux agents du FSB impliqués d'accéder à 500 millions de comptes utilisateurs de Yahoo !, après un premier piratage en 2013 qui aurait concerné près d'un milliard d'internautes.
Lire l'article

2.10 Cybersécurité : l'autre enjeu des big data

Les objets connectés captent toujours plus de données mais ne sont pas toujours correctement sécurisés.Pour les sécuriser, l'impensable doit être imaginé dès la conception des produits.

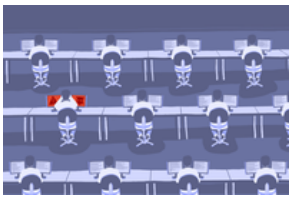
Lire l'article

2.11 Les moyens légaux de lutte contre la cybercriminalité

Qu'est ce que la cybercriminalité et comment la combattre ? Les réponses de Jean Harivel (Université Paris I, Panthéon Sorbonne) en vidéo, fait le point de manière très pédagogique sur les aspects juridiques de la cybercriminalité.

Voir la vidéo

2.12 Comment rendre efficace l'arsenal juridique français contre la cybercriminalité ?



Dans un rapport, deux associations, Cyberlex et le Centre expert contre la cybercriminalité français (CECyF), se sont penchés sur les modifications à apporter au code pénal français pour mieux prendre en compte la cybercriminalité. L'objectif poursuivi est d'offrir une lecture rigoureuse de l'ensemble du code pénal afin d'identifier les opportunités d'harmonisation et éventuellement d'amélioration dans la lutte contre la cybercriminalité.
Lire l'article

2.13 La cybersécurité restera une priorité nationale

Dans une interview, un porte-parole du Ministère de la défense fait le point sur l'essor des formations et des emplois dans le domaine de la défense en cas d'attaque informatique.

Lire l'article

2.14 Cybersécurité et collectivités territoriales

Lors de l'édition 2017 du Forum International de la cybersécurité, trois spécialistes ont été interviewés sur la question de la cybersécurité dans les collectivités territoriales. Une transcription de cette vidéo est disponible sur le site de l'April.

Voir la vidéo

3. PERSPECTIVES

3.1 Comprendre les grands principes de la cryptologie et du chiffrement

Historiquement, la cryptologie correspond à la science du secret, c'est-à-dire au chiffrement. Aujourd'hui, elle s'est élargie au fait de prouver qui est l'auteur d'un message et s'il a été modifié ou non, grâce aux signatures numériques et aux fonctions de hachage.
À l'occasion du mois européen de la cybersécurité, la CNIL vous explique ce que c'est et à quoi ça sert.

Lire l'article

3.2 Faut-il plus de cybersécurité, de cyberdéfense ou de cyber-renseignement ?

Aujourd'hui nous subissons, que ce soit dans le domaine économique/privé ou politique/public une quantité telle d'attaques qu'il est difficile de faire autrement que réagir. Les enjeux financiers ou électoraux, quand il ne s'agit pas des opérations extérieures, font que les autorités mobilisent des

moyens de plus en plus importants, même s'il est parfois difficile d'attribuer la cyberattaque à telle ou telle partie. S'agit-il seulement de réagir, de se prémunir ou d'anticiper les attaques dans le domaine cyber, dans une dimension parfois perçue comme virtuelle, mais dont l'impact est concret dans les domaines économiques, militaires et diplomatiques ?
Lire l'article

3.3 La mallette CyberEdu

Le projet CyberEdu a pour objectif d'introduire les notions de sécurité dans l'ensemble des formations dans le domaine du numérique en France. L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a passé un marché avec l'Université européenne de Bretagne (qui regroupe 28 établissements d'enseignement supérieur et de recherche) et Orange pour la réalisation de livrables à destination des responsables de formation et/ou des enseignants en informatique.
Consultez la mallette CyberEdu

POUR RESTER INFORMÉ.E

Comptes twitter d'éduscol et de la Direction du numérique pour l'éducation

Pour suivre l'actualité du site d'information des professionnels de l'éducation, rendez-vous sur twitter sur le compte @éduscol et sur celui de la DNE @Edu_Num.

Vous pouvez rester informé des dernières actualités du site éduscol Économie et gestion en vous abonnant au flux RSS général de la discipline ainsi qu'à celui de la lettre Édu_Num.

Cette lettre est proposée par la Direction du numérique pour l'éducation (DNE A2 - économie et gestion) et Christine Gaubert-Macon, Inspectrice générale, doyenne du groupe économie et gestion.