Cybersécurité : Aller plus loin dans la formation des salariés

Cybersécurité : Aller plus loin dans la formation des salariés

Alors que les entreprises sont de plus en plus sensibilisées aux risques de failles, de mise hors service de leurs systèmes (attaques DDOS) et de destruction de leurs données (via des ransomwares), elles ne pensent pas forcément que leurs outils de communication unifiée sont également concernés par les règles de protection.

• **Le chiffrement** : toutes les données, qu'elles soient stockées ou en transmission, doivent être protégées, les premières avec au minimum un chiffrement AES 128 bits et les secondes en ajoutant au moins le protocole TLS. Point important : il faut bien évidemment que les messages de tous les interlocuteurs, externes compris, soient cryptés.

• **Le pare-feu** : attention à ne pas tomber dans le piège d'une solution qui exposent des applications, des serveurs ou des équipements hors du pare-feu. De plus, il faut s'assurer que les solutions gèrent correctement le parcours des données au travers des serveurs d'authentification déjà en place.

• **Les mises à jour** : puisque les mises à jour de firmwares et autres logicielles corrigent essentiellement des vulnérabilités ou apportent des dispositifs de sécurité plus robustes, il est primordial qu'elles se fassent de manière automatique pour s'assurer que le SI est protégé le plus tôt possible. Une des approches consiste à passer par une solution en Cloud, automatiquement mise à jour par le fournisseur lui-même **mais à manier avec précaution car si vous avez déjà opté pour le Cloud, avez-vous la certitude que seuls les utilisateurs autorisés accèdent à cet espace de stockage externalisé ? Qui peut bien se connecter pendant que vous dormez ?**

• **La sécurité physique** : où se situent les données que stocke la solution de communication ? Il est essentiel d'avoir la garantie que le datacenter du fournisseur soit protégé 24/7 et qu'il soit régulièrement audité et protégé contre les intrusions physiques.

• **Changer les paramètres par défaut** : Changer tous les identifiants et mots de passe de ceux proposés par défaut pour quelque chose de plus complexe est une règle d'or en matière de cybersécurité.
« Parmi les nombreuses cyberattaques survenues en 2016, la plus célèbre fut celle lancée par le botnet Mirai qui ciblait les webcams. Or, si cette attaque a autant réussi, c'est parce que les mots de passe administrateurs par défaut de ces équipements étaient toujours actifs », dit-il.

• **Sécuriser le réseau, jusqu'aux utilisateurs** : Un segment non sécurisé du réseau est une porte d'entrée par laquelle peuvent passer les cyber-attaques pour atteindre tout le SI d'une entreprise. Les méthodes pour sécuriser le réseau comprennent l'application de restrictions d'accès, le blocage au niveau du pare-feu de certaines pièces attachées et le test régulier des failles de sécurités connues. Mais Gustavo Villardi prévient qu'il ne s'agit là que de résoudre une partie du problème. « Selon une étude récente menée par Verizon sur les failles de sécurité, l'erreur humaine continue d'être la cause principale des cyber-attaques. Les collaborateurs sont le maillon faible et les entreprises se doivent de former leur personnel pour qu'ils restent protégés en ligne et depuis quelque appareil que ce soit », témoigne-t-il.

• **L'usage à domicile** : les collaborateurs en télétravail ne bénéficient pas de l'encadrement de la DSI pour sécuriser leur accès domestique. Il est donc nécessaire de leur indiquer comment sécuriser une box pour activer le chiffrement du Wifi et passer par un VPN.

• **Les mots de passe** : des bonnes pratiques doivent être appliquées pour que les mots de passe de chaque salarié soient impossibles à deviner ; cela comprend aussi bien de la complexité dans l'enchaînement des caractères que la fréquence de remplacement des mots de passe.

• **L'accès** : les collaborateurs devraient toujours éteindre un équipement lorsqu'ils ne s'en servent pas, afin d'éviter que quelqu'un ne se connecte sur les services restés ouverts

• **Le mode privé** : l'utilisation d'un système de visioconférence uniquement avec les paramètres du mode privé évite que quelque des personnes extérieures puissent se greffer sur une conférence.

[lire l'intégralité de l'article source]

Réagissez à cet article

Source : *Cybersécurité : les trois mesures à prendre pour protéger la communication unifiée – Global Security Mag Online*

Dispositif biométrique d'accès à la cantine : quelles formalités à la CNIL ? | Denis JACOPINI

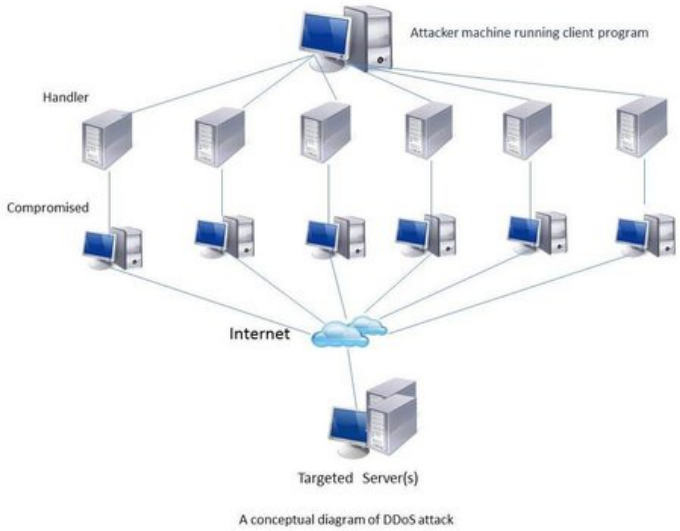
Dispositif biométrique d'#accès à la cantine : quelles formalités à la CNIL ?

Les dispositifs biométriques utilisant le contour de la main des élèves pour gérer l'accès à la cantine scolaire sont couverts par une autorisation unique adoptée par la CNIL.

Les établissements qui souhaitent installer ce type de dispositifs doivent faire une déclaration simplifiée, en sélectionnant dans l'onglet « Finalité » l'autorisation unique AU-009.
Le responsable du dispositif s'engage ainsi à se conformer aux caractéristiques décrites dans ce texte.
Les autres dispositifs biométriques (réseaux veineux, empreintes digitales, reconnaissance faciale, etc.) doivent faire l'objet d'une demande d'autorisation préalable auprès de la CNIL.

Source :
http://www.aide.cnil.fr/selfcnil/site/template.do;jsessionid=D5FEF7DD5664BF01E19E95AF8AF7782F

Comment se protéger des attaques DDoS ? | Denis JACOPINI



A conceptual diagram of DDoS attack

Comment se protéger des attaques DDoS ?

Les entreprises doivent arrêter de compter sur leurs fournisseurs de services Internet pour les protéger des attaques DDoS et doivent prendre les choses en main.

Les attaques par Déni de Services Distribués (DDoS) sont l'une des menaces Internet les plus anciennes et continuent d'être le principal risque pour les réseaux à travers le monde. En même temps que les protections ont évolué, la technologie utilisée par les hackers s'est adaptée et est devenue beaucoup plus sophistiquée. De nouveaux types d'attaques ciblent désormais les applications et services, et sont souvent cachés dans les couches 3 et 4, ce qui les rend difficilement détectables.
En matière d'attaques DDoS, le secteur financier est l'une des cibles privilégiées des cybercriminels, suivie de près par le secteur public. Outre le fait de perturber les opérations Internet par un assaut brutal de données, les attaques DDoS ont récemment été utilisées pour recueillir des informations financières et relatives au commerce en ligne. Ces attaques ont souvent pour objectif de perturber les opérations, principalement en détruisant l'accès à l'information.
Il y a généralement trois catégories de motivations derrière les attaques DDoS: politique, de représailles et financière. Les attaquants politiques ciblent ceux qui ne sont pas d'accords avec leurs convictions politiques, sociales ou religieuses. Lorsqu'un botnet ou un important réseau cybercriminel est démantelé, cela peut déclencher des attaques de représailles contre ceux qui ont aidé ou assisté les autorités. Les attaques motivées par l'argent suivent un schéma « pay-to-play » dans lequel les hackers sont compensés par une tierce partie qui leur demande de mener l'attaque pour elle. Quelle que soit la motivation, le résultat est le même – votre réseau et services en ligne deviennent indisponibles, et peuvent rester ainsi pendant un long moment.

Méfiez-vous des attaques DDoS avancées visant la couche applicative
Il existe de nombreux types d'attaque DDoS largement utilisés aujourd'hui, allant des anciennes méthodes des débuts de l'Internet aux dernières attaques avancées visant la couche 7 et ciblant les applications. L'inondation de requêtes SYN et HTTP GET sont les plus communes et utilisée pour surcharger les connexions réseau ou les serveurs derrière les pare-feu et système de prévention d'intrusion (IPS).

Toutefois, le plus inquiétant est que les attaques visant la couche applicative utilisent des mécanismes beaucoup plus sophistiqués pour attaquer les services et réseau des organisations. Plutôt que d'inonder simplement un réseau avec du trafic ou des sessions, ces types d'attaques ciblent des services et applications spécifiques pour épuiser lentement les ressources au niveau de l'application (couche 7).
Les attaques visant la couche applicative peuvent être très efficaces en utilisant peu de volumes de trafic, et peuvent être considérer comme tout à fait normales par la plupart des méthodes de détection DDoS traditionnelles. Cela rend les attaques visant la couche applicative beaucoup plus difficiles à détecter que les autres types d'attaque DDoS basiques.

Les options en matière de protection DDoS
La plupart des FAI offrent une protection DDoS des couches 3 et 4 pour empêcher les liens des organisations d'être inondés lors d'attaques volumétriques de masse. Cependant, ils n'ont pas la capacité de détecter les plus petites attaques visant la couche 7. Ainsi, les centres de données ne devraient pas uniquement compter sur leur FAI pour bénéficier d'une solution complète DDoS, dont la protection de la couche applicative. Au lieu de cela, ils devraient envisager de mettre en place une des mesures suivantes:
1. Les fournisseurs de services DDoS: Il existe beaucoup de solutions hébergées DDoS basées sur le cloud qui fournissent des services de protection des couches 3, 4 et 7. Elles vont des projets peu couteux pour les petits sites Web jusqu'à ceux pour les grandes entreprises qui requièrent la couverture de plusieurs sites Web. Elles sont en général très faciles à mettre en place et fortement poussées auprès des petites et moyennes entreprises. La plupart offre des options de tarification personnalisée et beaucoup ont des services de détection avancée de la couche 7 à disposition des grandes organisations qui nécessitent que des capteurs soient installés dans le centre de données. Beaucoup d'entreprises choisissent cette option, mais certaines d'entre elles doivent faire face à des frais excédentaires importants et imprévus lorsqu'elles sont frappées par des attaques DDoS en masse. Par ailleurs, la performance n'est parfois pas à la hauteur car les fournisseurs de services redirigent le trafic DDoS vers les centres de protection au lieu de les stopper en temps réel, ce qui est particulièrement problématique pour les attaques de courte durée, qui sont celles généralement rencontrées.
2. Pare-feu ou IPS: Presque tous les pare-feux et systèmes de prévention d'intrusion (IPS) modernes revendiquent un certain niveau de défense DDoS. Les pare-feu nouvelles générations avancés (NGFW) offrent des services DDoS et IPS et peuvent protéger de nombreuses attaques DDoS. Avoir un dispositif pour le pare-feu, IPS et DDoS est plus facile à gérer, mais il peut être submergé par des attaques volumétriques DDoS, et peut ne pas avoir les mécanismes sophistiqués de détection pour la couche 7 que d'autres solutions ont. Un autre compromis à prendre en compte est que l'activation de la protection DDoS sur le pare-feu ou l'IPS peut impacter la performance globale du seul dispositif, entrainant des débits réduits et une augmentation de la latence pour les utilisateurs finaux.
3. Appliances dédiées à la protection d'attaques DDoS: Ce sont des dispositifs matériels qui sont déployés dans un centre de données et utilisés pour détecter et stopper les attaques DDoS basiques (couche 3 et 4) et avancées (couche 7). Déployées au point d'entrée principal pour tout le trafic Web, ces appliances peuvent à la fois bloquer les attaques volumétriques en masse et surveiller tout le trafic entrant et sortant du réseau afin de détecter les comportements suspects des menaces visant la couche 7. En utilisant un dispositif dédié, les dépenses sont prévisibles car le coût est fixé quelle que soit la fréquence des attaques, que l'entreprise soit attaquée une fois en six mois ou tous les jours. Les aspects négatifs de cette option sont que ces dispositifs sont des pièces matérielles supplémentaires à gérer, que les unités à faible bande passante peuvent être submergées lors d'attaques volumétriques en masse, et que de nombreux fabricants nécessitent des mises à jour fréquentes en matière de signatures.
Les solutions matérielles dédiées de protection des attaques DDoS existent en deux versions principales – celle pour les opérateurs télécoms et celles pour les entreprises. Les premières sont des solutions complètes conçues pour les réseaux mondiaux des FAI et sont très coûteuses. La plupart des organisations qui veulent protéger leurs centres de données privés optent habituellement pour les modèles entreprises qui offrent une détection et protection DDoS rentable. Les modèles d'aujourd'hui peuvent gérer des attaques volumétriques en masse et assurer une protection à 100% des couches 3, 4 et 7 ou peuvent être utilisés pour compléter une protection fournie par le FAI contre les attaques DDoS en masse et assurer une détection et protection avancées de la couche 7. Bien que ces dispositifs nécessitent un investissement initial, ce qui n'est pas le cas des solutions hébergées, ils sont généralement beaucoup moins chers à long terme si l'on prend en compte les frais excédentaires dans le budget total.

Les entreprises devraient considérer des appliances de protection d'attaques DDoS qui utilisent des méthodes d'adaptation basées sur le comportement pour identifier les menaces. Ces appliances apprennent les bases de référence de l'activité normale des applications et ensuite surveillent leurs trafics par rapport à ces bases. Cette approche d'adaptation/apprentissage a l'avantage de protéger les utilisateurs des attaques zero-days inconnues puisque que le dispositif n'a pas besoin d'attendre que les fichiers signatures soient mis à jour.
Les attaques DDoS sont en hausse pour presque toutes les organisations, grandes ou petites. Les menaces potentielles et volumes augmentent à mesure que de plus en plus d'appareils, y compris les téléphones mobiles, accèdent à Internet. Si votre organisation a une propriété Web, la probabilité de subir une attaque n'a jamais été aussi élevée.
La nature évolutive des attaques DDoS signifie que les entreprises ne peuvent plus compter uniquement sur leur FAI pour se protéger. Les organisations doivent commencer à effectuer des changements dès à présent pour une plus grande prévoyance et bénéficier de défenses plus proactives pour les services au niveau des applications et du réseau.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.journaldunet.com/solutions/expert/59977/comment-se-proteger-des-attaques-ddos.shtml

---

Attaque informatique : les 7 gestes qui sauvent

Attaque informatique : les 7 gestes qui sauvent

Perspectives IT, 14 octobre 2016, 11:00SÉCURITÉ 3 1 10BLOG PROPOSÉ PAR DELL EMCVotre PC est infecté. Mais repérer l'attaque n'est que la première étape. Il faut ensuite organiser la réponse à incident. Et les premiers gestes ont ici une importance capitale.

7 gestes de premiers secours à connaître face à une attaque informatique.

Votre poste de travail est infecté. La stratégie en place de détection des intrusions a fonctionné et une menace a été identifiée. Et ensuite ? Repérer l'attaque informatique n'est que la première étape. Encore faut-il savoir ensuite organiser la réponse à incident. Et les premiers gestes ont ici une importance capitale. Pour éviter que la situation ne s'aggrave tout d'abord, mais aussi pour permettre de récolter un maximum d'informations sur l'attaque. Les collaborateurs d'une entreprise n'étant pas censés être tous des experts en sécurité informatique, la formation et la sensibilisation sont des missions clés des RSSI. Pour les aider, le CERT-FR a dressé une liste des bons réflexes à adopter.

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves 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 Cybersécurité & Conformité Contactez-nous

Réagissez à cet article

Source : *Attaque informatique : les 7 gestes qui sauvent – Silicon*

RGPD : Qu'est-ce qu'une donnée à caractère personnel ?

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

LE NET EXPERT AUDITS & EXPERTISES | EXPERTISES DE SYSTÈMES DE VOTES ELECTRONIQUES LENETEXPERT.fr | RGPD CYBER LE NET EXPERT MISES EN CONFORMITÉ | SPY DETECTION Services de détection de logiciels espions | LE NET EXPERT FORMATIONS | LE NET EXPERT ARNAQUES & PIRATAGES

RGPD : Qu'est-ce qu'une donnée à caractère personnel ?

L'entrée en vigueur, en mai dernier, du Règlement UE 2016/679 (RGPD [1]), a donné un souffle nouveau à la protection des données des consommateurs et usagers d'internet en France et en Europe. Mais si on entend beaucoup parler de données personnelles, il n'est pas toujours facile de savoir précisément ce qu'il faut entendre par cette notion.

Le règlement (article 4) les défini comme étant *toute information se rapportant à une personne physique identifiée ou identifiable*.

Le règlement précise également ce qu'est une personne physique identifiable : *une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale*.

En pratique, il faut comprendre de cette définition que, toute donnée se rapportant à votre personne et permettant, même indirectement de vous identifier est une donnée personnelle.

Ainsi, votre nom, prénom, âge, date et lieu de naissance, une photo de vous, un pseudonyme, un numéro de téléphone ou de sécurité sociale, une adresse IP, etc. constituent des données à caractère personnel.

…[lire la suite]

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 : *Qu'est-ce qu'une donnée à caractère personnel ? – Force Ouvrière*

Mon employeur peut-il enregistrer ou écouter mes conversations téléphoniques à mon insu ? | Denis JACOPINI

Mon employeur peut-il enregistrer ou écouter mes conversations téléphoniques à mon insu ?

Un employeur n’a le droit ni d’enregistrer ni d’écouter les conversations téléphoniques de ses employés s’ils n’en sont pas informés.S’il le fait, il commet un délit et risque des sanctions pénales.

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l’hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.
Besoin d’informations complémentaires ?
Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu’intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d’entreprise.
Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

S o u r c e : http://www.aide.cnil.fr/selfcnil/site/template.do;jsessionid=4FBDF806985B62BC62EB3DEBC567BF6F?name=Mon+employeur+peut-il+enregistrer+ou+%C3%A9couter+mes+conversations+t%C3%A9l%C3%A9phoniques+%C3%A0+mon+insu+%3F&id=106

Quelles formalités pour transféret des données personnelles hors UE ? | Denis JACOPINI

Quelles formalités pour transféret des données personnelles hors UE ?

Quelles formalités accomplir auprès de la CNIL si vous transférez des données personnelles hors de l'Union européenne ?
Les formalités à accomplir auprès de la CNIL varient en fonction :
• du régime juridique applicable au traitement principal (déclaration normale ou autre formalité),
• de la désignation d'un correspondant informatique et libertés,
• du pays de destination,
• du cadre juridique du transfert.

1.
Certains transferts sont dispensés de déclaration
Les traitements mis en œuvre sur le territoire français par des prestataires agissant pour le compte de responsables de traitement établis hors de l'UE et concernant des données personnelles collectées hors de l'UE sont dispensés de formalité, à condition que les traitements aient pour finalité : la gestion des rémunérations, la gestion du personnel ou la gestion des fichiers de clients et de prospects (Dispense n° 15)

2.
Certains transferts hors UE bénéficient déjà d'une autorisation de la CNIL,
C'est notamment le cas des normes suivantes :
• Norme simplifiée n°NS-046 (gestion du personnel)
• Norme simplifiée n°NS-048 (gestion clients-prospects)
• Autorisation unique n°AU-004 (alertes professionnelles)
• Des transferts bénéficiant d'une autorisation unique BCR

3.
Dans les autres cas
Complétez le formulaire correspondant au régime juridique de formalités CNIL applicable au traitement principal envisagé (déclaration normale ou une autre formalité).
Dans ce formulaire, dans l'onglet « Transferts », sélectionnez « **Transmission de données Hors UE** ».

CADRE JURIDIQUE DU TRANSFERT	SI LE TRAITEMENT PRINCIPAL RELÈVE DE LA DÉCLARATION	SI LE TRAITEMENT PRINCIPAL RELÈVE DE L'AUTORISATION	SI LE TRAITEMENT PRINCIPAL RELÈVE DE LA DEMANDE D'AVIS
Le transfert se fait dans un pays présentant une protection suffisante ou Recours aux exceptions	Remplir le formulaire de déclaration normale et l'annexe transferts Ou si l'organisme a désigné un CIL : Inscription au registre du CIL	Remplir le formulaire de demande d'autorisation et l'annexe transferts	Remplir le formulaire de demande d'avis et l'annexe transferts
Clauses contractuelles types	Remplir le formulaire de déclaration normale et l'annexe transferts Le transfert est soumis à l'autorisation préalable de la CNIL	Remplir le formulaire de demande d'autorisation et l'annexe transferts	Remplir le formulaire de demande d'avis et l'annexe transferts
« Binding corporate rules » (BCR) au sein d'un même groupe	Remplir le formulaire de déclaration normale et l'annexe transferts Le transfert est soumis à l'autorisation préalable de la CNIL	Remplir le formulaire de demande d'autorisation et l'annexe transferts	Remplir le formulaire de demande d'avis et l'annexe transferts

Comment procéder ?
• 1 – Complétez le formulaire
• 2- Sélectionnez les pays destinataires
• 3 – Remplissez l'annexe Transfert
• 4 – L'instruction du transfert par la CNIL

Attention ! si vous transférez des données pour plusieurs finalités distinctes, vous devez créer une annexe pour chaque transfert hors UE.
(ex : finalités d'hébergement de données et finalité de saisie de données = 2 annexes).
En revanche, une seule « annexe transfert » suffit pour plusieurs destinataires dès lors que la finalité du transfert est la même.

Article original de la CNIL

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 : Transferts hors UE : quelles formalités ? | CNIL

4 conseils pour éviter les cyber-attaques pendant les soldes | Denis JACOPINI

4 conseils pour éviter les cyber-attaques pendant les soldes

Période propice aux achats en ligne, les soldes sont aussi prisées par les cybercriminels. Tour d'horizon des mesures à prendre pour se prémunir d'une attaque informatique.

Les soldes d'hiver démarrent aujourd'hui. Période de forte activité, les e-commerçants vont voir leurs ventes augmenter et cela ne manquera pas d'attirer les cybercriminels en tout genre. A cette période, chaque année, les entreprises tout comme les particuliers sont la cible de nombreuses tentatives de piratage, cependant quelques conseils simples peuvent éviter aux particuliers les arnaques.

Pendant un mois les soldes représente un pic d'activité pour les sites d'achats en ligne. Début 2014, selon une étude de la Fevad (Fédération du e-commerce et de la vente à distance) et du CSA, 7 internautes sur 10 envisageaient de préparer ou de faire leurs achats en ligne pendant les soldes. Parmi eux, 26% envisageaient d'effectuer leurs achats via smartphones. L'occasion idéale pour les pirates informatiques en quête de nouvelles victimes !

Pour se prémunir de ces attaques, les internautes peuvent prendre quelques précautions simples mais pourtant essentielles :
1. Veiller à toujours avoir les dernières mises à jour de ses applications, de son système d'exploitation et des logiciels de sécurité. Des failles sont régulièrement enregistrées et les correctifs sont présents dans les mises à jour, mais encore faut-il les effectuer !

2. S'en tenir aux règles d'or : Ignorer ou bloquer les pop-ups, utiliser un mot de passe original et sécurisé (aux oubliettes le 0000 ou le 1234), commander sur des sites fiables et via des connexions sécurisées en https.
3. Eviter de cliquer sur les liens directement depuis un emailing :le phishing reste à la mode, et il est particulièrement efficace en période de soldes lorsque des dizaines d'emails vous propose leurs bons plans quotidiennement. Si une offre est pertinente : mieux vaut retaper l'adresse sur son navigateur afin d'éviter tout soucis.
4. Eviter les transactions depuis des réseaux Wi-Fi publics. La plupart des réseaux publics (gares, cafés, etc) ont un niveau de cryptage faible, et donc une moindre sécurité. Les informations bancaires pourraient atterrir dans les mains d'une tierce personne. Que l'on soit connecté depuis un ordinateur, une tablette, ou un mobile, mieux vaut donc se méfier des réseaux ouverts.

Autre point sensible : Les achats via smartphones et tablettes sont de plus en plus communs, mais il est important de se méfier lors de son shopping. En effet, ces terminaux font face à de nombreuses menaces et sont souvent moins bien sécurisés que les ordinateurs.
Ici aussi des règles d'or s'appliquent : ne pas télécharger d'applications gratuites et de propriétaires inconnus sur internet afin d'éviter les trojans, acheter et visualiser les comptes seulement via des applications propriétaires (celles de sa banque ou celles d'e-commerçants), supprimer l'historique de navigation, le cache et les cookies régulièrement afin de supprimer les données sensibles.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.lesechos.fr/idees-debats/cercle/cercle-120665-4-conseils-pour-eviter-les-cyber-attaques-pendant-les-soldes-1080620.php

Formation RGPD pour devenir DPO de votre organisme – Prochaine formation les 17 18 et 19 septembre 2018 à Paris

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

Depuis le 25 mai 2018, le RGPD (Règlement européen sur la Protection des Données) est applicable. De nombreuses formalités auprès de la CNIL ont disparu. En contrepartie, la responsabilité des organismes est renforcée. Ils doivent désormais assurer une protection optimale des données à chaque instant et être en mesure de la démontrer en documentant leur conformité.

Formation pour DPO « Je veux devenir le Délégué à la Protection des Données de mon établissement » : 2 jours (Mettez en place une démarche de mise en conformité RGPD)

Que vous soyez bientôt ou soyez déjà désigné « Délégué à la Protection des Données » ou « DPO », nous vous conseillons cette formation. Cette formation vous permettra de rentrer en profondeur dans le Règlement Européen et vous présentera des éléments concrets afin de mettre en place durablement une mise en conformité avec le RGPD au sein de votre établissement.
Consultez les prochaines dates d'animation autour de chez vous ?

Je me présente : Denis JACOPINI. Je suis Expert de justice en informatique **spécialisé en cybercriminalité et en RGPD (protection des Données à Caractère Personnel)**, consultant depuis 1996 et formateur depuis 1998. J'ai bientôt une expérience d'une dizaine d'années dans la mise en conformité avec la réglementation relative à la Protection des Données à Caractère Personnel. De formation d'abord technique, Correspondant CNIL (CIL : Correspondant Informatique et Libertés) puis récemment Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur, il m'est ainsi aisé d'expliquer le coté pragmatique de la démarche de mise en conformité avec le RGPD.
« Mon objectif est de vous transmettre mon savoir, vous dévoiler mes techniques mes outils car c'est bien ce que les personnes qui souhaitent s'inscrire à une formation RGPD attendent. »

Votre Prénom / NOM (obligatoire)

Votre adresse de messagerie (obligatoire)

Un numéro de téléphone (pour faciliter l'organisation)

Vous souhaitez avoir des informations sur :
☐- la formation « Comprendre le RGPD » : 1 jour
☐- la formation « Je veux devenir Délégué à la Protection des Données » 2 jours
☐- la formation « Je mets en conformité mon établissement » 3+1 jours
☐- la formation « Mise en conformité RGPD sur mesure »
☐- un accompagnement personnalisé au RGPD

Vous souhaitez réserver une ou plusieurs place(s) à la formation :

Formation pour TPE/PME : **« Comprendre le RGPD et ce qu'il faut savoir pour bien démarrer »**

Pas de date de prévue pour l'instant.
Face à une importante demande en formations et en accompagnements personnalisés ou individuels, nous avons momentanément interrompu l'organisation de formations de groupe.
Nous sommes néanmoins à votre entière disposition si vous souhaitez organiser une formation dans vos locaux.
N'hésitez pas à nous faire part de vos besoins et voyons ensemble si nous pouvons vous trouver une solution.

Formation pour DPO : **« Je veux devenir le Délégué à la Protection des Données de mon établissement »**

Pas de date de prévue pour l'instant.
Face à une importante demande en formations et en accompagnements personnalisés ou individuels, nous avons momentanément interrompu l'organisation de formations de groupe.
Nous sommes néanmoins à votre entière disposition si vous souhaitez organiser une formation dans vos locaux.
N'hésitez pas à nous faire part de vos besoins et voyons ensemble si nous pouvons vous trouver une solution.

Formation pour consultants : **« J'accompagne mes clients dans leur mise en conformité avec le RGPD »**

Pas de date de prévue pour l'instant.
Face à une importante demande en formations et en accompagnements personnalisés ou individuels, nous avons momentanément interrompu l'organisation de formations de groupe.
Nous sommes néanmoins à votre entière disposition si vous souhaitez organiser une formation dans vos locaux.
N'hésitez pas à nous faire part de vos besoins et voyons ensemble si nous pouvons vous trouver une solution.

☐Autre ville ou sujets souhaités en individuel (indiquez ci-dessous)

Votre message avec vos préférences de date ou vos commentaires

Envoyer

Nos formations s'organisent en groupe. Le lieu de la formation sera facilement accessible à Métro à Paris, facilement accessible en tramway à Lyon et à proximité d'une gare TGV et disposera d'un parking à Marseille. Votre place ne sera réservée qu'à la réception de votre acompte. Si la formation était annulée (nombre de participants insuffisants ou en cas de force majeure), votre acompte sera remboursé en intégralité dans les 5 jours (les chèques seront encaissés à partir du jour de la formation). En cas d'annulation de votre part moins de 48 heures avant la formation, l'acompte pourra ne pas être remboursé car destiné à régler les frais de réservation de salle et d'organisation, eux même non remboursables.

Accompagnant depuis 2012 de nombreux établissements, Denis JACOPINI, Expert informatique diplômé en cybercriminalité, certifié en gestion des risques sur les systèmes d'information (ISO 27005) et formé par la CNIL depuis 2011 sur une trentaine de thèmes, est en mesure de vous accompagner dans votre démarche de mise en conformité RGPD.

DÉSIGNATION
N° DPO-15945

Numéro de formateur
93 84 03041 84
Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Datadock
Organisme validé et référencé

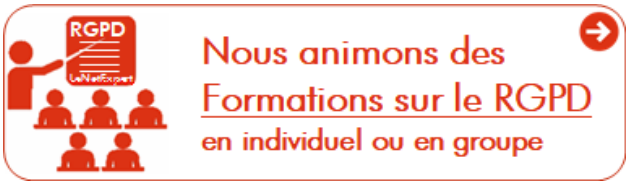
Besoin d'un expert pour vous mettre en conformité avec le RGPD ?

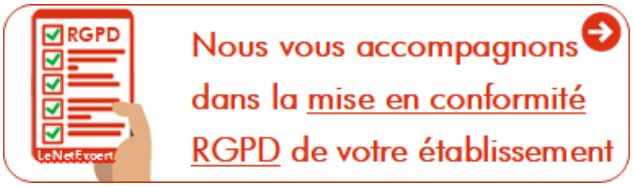
Contactez-nous

Accompagné de son équipe d'auditeurs et de formateurs, notre Expert, Denis JACOPINI est spécialisé en cybercriminalité et en protection des Données à Caractère Personnel, formateur depuis 1998 et consultant depuis 1996. Avec bientôt une **expérience d'une dizaine d'années** dans la mise en conformité avec la réglementation relative à la Protection des Données à Caractère Personnel, de formation d'abord technique, Correspondant CNIL en 2012 (CIL : Correspondant Informatique et Libertés) puis en 2018 Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur, il lui est ainsi aisé d'accompagner les organismes dans leur démarche de **mise en conformité avec le RGPD**.

« Mon objectif, vous assurer une démarche de mise en conformité validée par la CNIL. ».

Nous vous aidons à vous mettre en conformité avec le RGPD de 2 manières :





Quelques articles sélectionnés par nos Experts :

Comment se mettre en conformité avec le RGPD
Accompagnement à la mise en conformité avec le RGPD de votre établissement
Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles
Comment devenir DPO Délégué à la Protection des Données
Des guides gratuits pour vous aider à vous mettre en conformité avec le RGPD et la CNIL
Mise en conformité RGPD : Mode d'emploi
Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016
DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016
Comprendre le Règlement Européen sur les données personnelles en 6 étapes
Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

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

Source : Denis JACOPINI et *Règlement européen : se préparer en 6 étapes*

Mon employeur peut-il enregistrer ou écouter mes conversations téléphoniques professionnelles ? | Denis JACOPINI

Mon employeur peut-il enregistrer ou écouter mes conversations téléphoniques professionnelles ?

Votre employeur peut mettre en place un dispositif d'écoute ou d'enregistrement des conversations téléphoniques professionnelles.

Ce dispositif doit toutefois prévoir des garanties :

• Écoute ou enregistrement ponctuel, d'une partie seulement des appels;
• Écoute ou enregistrement à des fins d'évaluation, de formation et de contrôle qualité ;
• Information et consultation préalables des instances représentatives du personnel et des employés ;
• Conservation limitée à un an maximum des enregistrements audio ;
• Déclaration à la CNIL du dispositif.

Dans certains cas prévus par un texte légal, des enregistrements permanents peuvent être imposés (services d'urgence ou ordres boursiers, par exemple).

Source :
http://www.aide.cnil.fr/selfcnil/site/template.do;jsessionid=ED8EEF20B4B0A650CC53FA8D4DE31A0C?name=Mon+employeur+peut-il+enregistrer+ou+%C3%A9couter+mes+conversations+t%C3%A9l%C3%A9phoniques+professionnelles+%3F&id=269