La Lettre de SecuriteOff
La sécurité informatique au service des PME/PMI !

Tous les 15 jours, découvrez La Lettre de SecuriteOff (envoyée par email au format PDF) consacrée à la réglementation liée aux usages numériques et à la sécurité informatique. Cette lettre professionnelle vous permet de connaître les informations indispensables à la pérennité de votre entreprise.

TOUTES les entreprises, quelles que soient leur taille et leur activité, peuvent être victimes d'une attaque informatique, car les données sont devenues la cible des escrocs.
Par ailleurs, les pirates passent systématiquement par des PME pour attaquer des grands groupes.

En matière de protection des données à caractère personnel, la réglementation devient de plus en plus contraignante et exigeante.
Ainsi, le nouveau Règlement européen (RGPD) n° 2016/679 du 27 avril 2016, sur la protection des données, applicable à compter de mai 2018, obligera toutes les entreprises à notifier les violations de données personnelles sous 72 heures.
Cette obligation s'adressera à toutes les entreprises et à leurs prestataires de services.

Voici un exemplaire regroupant des informations publiées dans plusieurs numéros de La Lettre de SecuriteOff.

La Lettre de SecuriteOff
La sécurité informatique au service des PME/PMI !

Sommaire

Droit et informatique
Les SMS sur des smartphones professionnels sont... « professionnels »..... page 2
Injure par email et dommages-intérêts..... page 3
Condamnation pour usurpation d'identité sur un réseau social..... page 3

Sécurité informatique
Mises à jour obligatoires : Internet Explorer..... page 3
Bonnes pratiques :
Augmentation des spams avec Office..... page 4
Attention aux rançongiciels..... pages 4 et 5

DROIT ET INFORMATIQUE

- **Les SMS sur des smartphones professionnels sont… « professionnels »**

Le 10 février 2015, la chambre commerciale de la Cour de cassation a rendu un arrêt qui donne aux SMS échangés sur les téléphones portables mis à disposition par les employeurs une présomption de « caractère professionnel ». Pour définir ces petits messages comme étant « privés », les salariés devront écrire les mots « personnel » ou « perso » au début du texte.

Pour la Cour de cassation, ces messages peuvent donc constituer des preuves recevables et leur lecture ne peut « être assimilée à l'enregistrement d'une communication téléphonique privée effectuée à l'insu de l'auteur des propos ».

Par contre, l'employeur ne peut mettre en place une surveillance constante et permanente de ses employés, sauf à justifier d'un risque particulier pour la sécurité des biens ou des personnes, tels que notamment des transferts de fonds, des installations dangereuses.

Pour rappel, depuis mai 2013 ainsi, l'employeur a le droit d'ouvrir, sans la présence du salarié, un email qui n'a pas été identifié comme « personnel ». Là aussi, le salarié doit indiquer la mention « personnel ». En clair, l'entreprise ne peut pas accéder à des emails « personnels » émis par les salariés et reçus par eux grâce à leur ordinateur professionnel, et ce, même même si elle en avait interdit une utilisation privée. Néanmoins, l'employeur peut demander au juge l'intervention d'un huissier pour accéder à ces emails. Le juge acceptera si cette désignation répond à un motif légitime (par exemple, un salarié est soupçonné de concurrence déloyale) et est nécessaire à la protection des droits de l'employeur.

Sans cette autorisation d'un juge, le licenciement d'une personne pour faute grave s'appuyant sur la lecture d'emails « personnels » sera jugé « sans cause réelle et sérieuse ».

- **Injure par email et dommages-intérêts**

Le 9 avril, le tribunal de grande instance de Paris a condamné un représentant du syndicat CGT EssoMobil à 3 000 euros de dommages et intérêts pour injure non publique dans un email. Inspiré par la Cour de cassation, le TGI a tenu compte du nombre de personnes auxquels le message litigieux a été diffusé ainsi que « l'intention de nuire » de son auteur.

- **Condamnation pour usurpation d'identité sur un réseau social**

Par un jugement en date du 24 mars 2015, le Tribunal correctionnel de Paris a condamné deux individus à des amendes de 4 000 et 3 000 euros avec sursis pour usurpation d'identité sanctionnée par l'article 226-4-1 du Code Pénal, ainsi qu'à verser solidairement la somme totale de 5 000 euros à la victime et sa compagne à titre de dommages-intérêts.
Les prévenus avaient dérobé le téléphone portable d'une personne sur son lieu de travail, puis avaient créé un faux profil Facebook sous ses nom et prénom pour y publier plusieurs photographies personnelles et des « termes vulgaires, en vue de troubler leur tranquillité et de leur nuire".

SÉCURITÉ INFORMATIQUE

- **MISE À JOUR OBLIGATOIRE**

- ✓ **Internet Explorer**

Le 10 mars 2015, Microsoft a publié 14 bulletins de sécurité, dont 5 sont considérés comme critiques et 9 comme importants :
Parmi celles-ci, douze vulnérabilités ont été corrigées au sein de Internet Explorer (bulletin MS15-018). Dix d'entre elles sont exploitables sur la dernière version du navigateur, dont huit qui permettent d'exécuter du code arbitraire à distance. Deux corruptions mémoire, identifiées par les vulnérabilités CVE-2015-1625 et CVE-2015-1634, permettent une exécution de code arbitraire à distance sur l'ensemble des versions du navigateur, d'Internet Explorer 6 à 11. Des attaques ont pu être observées pour 5 de ces vulnérabilités. Les deux autres vulnérabilités permettent une élévation de privilèges.

SecuriteOff

➢ BONNES PRATIQUES

✓ Augmentation des spams avec Office

Depuis le 8 juin 2015, il est observé à l'échelle nationale une vague de spams dont le taux de blocage par les passerelles antispam est relativement faible.
Ces spams embarquent des documents Microsoft Office contenant des macros VBA malveillantes. Ces macros ont pour but d'infecter la victime avec Dridex, qui est un logiciel malveillant de type bancaire.
Afin de se protéger contre ce type de menace, les conseils habituels sont rappelés :
- Ne pas ouvrir les documents ou les pièces jointes non sollicités ;
- Désactiver l'exécution automatique des macros dans les suites bureautiques ;
- Maintenir le système d'exploitation et l'antivirus à jour.

La désactivation de l'exécution automatique des macros se paramètre dans le menu suivant :
Fichier / Options / Centre de gestion de la confidentialité / Paramètre du Centre de gestion de la confidentialité / Paramètres des macros / Désactiver toutes les macros avec notifications.

✓ Attention aux rançongiciels (ou ransomwares)

Le CERT-FR a détecté une nouvelle variante dans la famille des rançongiciels : CryptoFortress. Ce programme malveillant arrive par les voies classiques de l'ingénierie sociale. Le plus souvent il s'agit d'une pièce jointe à un courriel. Une fois exécuté, il chiffre (il crypte) les fichiers de la victime avant d'exiger une rançon.

Le CERT-FR recommande les actions suivantes :
- Effectuer régulièrement des copies de sauvegarde sur des supports déconnectés ;
-Sensibiliser les utilisateurs : la plupart de ces messages sont non sollicités, d'un émetteur inconnu et contiennent des fautes d'orthographe ;
- Utiliser des restrictions logicielles notamment pour interdire l'exécution de code depuis les répertoires temporaires ;
- Mettre à jour les bases de signatures antivirus et des passerelles de messagerie ;
- Mettre en place une protection appropriée des partages de fichiers, notamment en positionnant les permissions en lecture seule lorsque c'est possible ;
- Appliquer les correctifs de sécurité (système d'exploitation et applications).

Si l’un de vos utilisateurs est victime de ce type de virus, le CERT-FR recommande la conduite suivante :
- Isoler au plus vite le poste compromis du réseau (fixe et sans fil);
- Identifier le message malveillant et rechercher d’éventuelles copies envoyées à d’autres destinataires afin de les supprimer ;
- Reformater le poste client et réinstaller un système sain ;
- Restaurer les copies de sauvegarde des fichiers perdus.

Le versement de la rançon à l’attaquant ne garantit ni le déchiffrement des fichiers ni la sécurité des moyens de paiement utilisés. Il peut notamment entraîner l’installation de virus supplémentaires sur le poste utilisé.

ABONNEZ-VOUS POUR NE RATER AUCUNE INFORMATION ESSENTIELLE À VOTRE ACTIVITÉ ÉCONOMIQUE

Pour vous abonner et recevoir par email (format PDF), tous les 15 jours, La Lettre de SecuriteOff, vous pouvez :

› soit envoyer un **virement bancaire** à SecuriteOff en indiquant comme objet « La Lettre de SecuriteOff » :
Banque populaire val de France
Compte : 30821440580
BIC : CCBPFRPPVER
IBAN : FR76 1870 7006 8030 8214 4058 037

Merci d'envoyer votre bulletin d'abonnement rempli à l'adresse email suivante : abonnement@securiteoff.com

› soit photocopier ce bulletin d'abonnement rempli et accompagné de votre **chèque** à l'ordre de SecuriteOff et l'envoyer par la Poste à l'adresse suivante :
13 rue Pierre de Ronsard
37540 Saint-Cyr-sur-Loire.

Une facture vous sera adressée dès réception de votre bulletin d'abonnement.

BULLETIN D'ABONNEMENT à *La Lettre de SecuriteOff*
Nom* :
Prénom* :
Entreprise ou organisme* :
Fonction* :
Adresse* :
Code postal* :
Ville* :
Email* :

* Mentions obligatoires

NOS TARIFS
* *Cochez la mention utile :*

O Je souhaite m'abonner pour **1 an**** (11 mois, 22 numéros) au prix de **83.33** € HT, soit 100 € TTC.

O Je souhaite m'abonner pour **6 mois** (12 numéros) au prix de **50 €** HT, soit 60 € TTC.

O Je souhaite m'abonner pour **3 mois** (6 numéros) au prix de **29.17 €** HT, soit 35 € TTC.

O Je souhaite m'abonner pour **1 mois** (2 numéros) au prix de **12.5 €** HT, soit 15 € TTC.

** Pas de lettre en août.

À PROPOS DE SECURITEOFF
Spécialisée dans la sécurité informatique avec des ingénieurs ayant 20 ans d'expérience, notre société, SecuriteOff, vous aide à renforcer la protection de votre entreprise.

- Nous vous proposons différents diagnostics et conseils.
- Nous vous apportons des solutions adaptées à vos besoins.

NOS 5 ATOUTS :

- Des services assurés par des Ingénieurs R&D en cybersécurité ayant 20 ans d'expérience.
- Une équipe pluridisciplinaire capable de répondre aux besoins spécifiques de toutes les PME.
- Des conseils et des solutions adaptés aux problématiques des PME.
- Une équipe à la pointe de la recherche (Laboratoire R&D) en attaques informatiques et en virus.
- Une équipe indépendante de tout éditeur de logiciels et de tout prestataire.

SecuriteOff est membre d'EDEN (European Defense Economic Network), cluster de 130 PME défense, sécurité et sûreté nationales.

VOTRE CONTACT :
Philippe Richard
Directeur de SecuriteOff.
Email : direction@securiteoff.com
Tél. : 06 85 63 43 27