La Police pourrait prochainement consulter vos données personnelles sur Facebook sans autorisation

	La Police pourrait prochainement consulter vos données personnelles sur Facebook sans autorisation

Face à la vague d'attentats qui frappe l'Europe, la Commission européenne discute actuellement de quelques changements dans les réglementations afin de permettre aux forces de Police d'accéder aux données des utilisateurs des services de Google et Facebook, sans autorisation préalable d'un Juge.

Les vagues d'attentat et la peur ambiante sont bien souvent l'occasion pour les gouvernements de voter des lois liberticides, et ce pourrait à nouveau être le cas dans toute l'Europe. La Commission européenne réfléchit actuellement à changer les réglementations afin de permettre aux forces de police d'aller piocher des informations dans les comptes des réseaux sociaux des utilisateurs, sans accord préalable de qui que ce soit.

Concrètement, le projet évoque même la possibilité pour les policiers d'origine étrangère de consulter les données privées des profils de ces réseaux sociaux, afin notamment d'enquêter sur un touriste ou une personne d'un autre pays de l'Union européenne. Exemple : vous partez en Italie pour quelques jours et vous faites arrêter par la police locale, ces derniers pourraient alors éplucher vos profils sociaux pour tenter d'obtenir plus d'informations sur vous, et ce, sans rien demander à la France.

Actuellement, trois projets de ce type ont été proposés et soumis à étude, l'un d'entre eux pouvant être adopté d'ici la fin de l'année 2018. Une des propositions évoque la possibilité de copier les données directement depuis le Cloud de la plateforme sociale afin d'en faire une sauvegarde et éviter la disparition des données en cas d'enquête…[lire la suite]

Commentaire de Denis JACOPINI

Entre Facebook qui analyse et espionne ses membres et les OPJ (Officiers de Police Judiciaire) qui peuvent consulter les données collectées par Facebook, il n'y a qu'un pas pour que ce même type de démarche soit aussi engagée auprès de Google pour qu'on nous mette des radars automatiques sur Internet qui nous flashent dès que quelqu'un en train picoler publie une photo.

Sans plaisanter, ces projets de loi consistent à permettre à des OPJ d'accéder aux zones privées de Facebook, car vous savez que lorsque vous publiez quelque chose sur Facebook, cet ajout peut être public (tout le monde peut le consulter et le voir) ou privé et il n'y a qu'un juge qui peut forcer Facebook à communiquer le contenu privé d'un compte. Ce projet ne changera rien pour ceux qui n'ont rien à se reprocher, et pas grand chose pour ceux qui ont quelques chose à se reprocher. Les OPJ pourrons disposer plus rapidement des contenus privés pour alimenter leurs enquêtes.

Il est fort probable à l'avenir qu'un autre réseau social soit utilisé par les malfrats l'histoire de faire courrier le chat…

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 RGPD (Protection des Données à Caractère Personnel).

- Audits RGPD
- Accompagnement à la mise en conformité RGPD
- Formation de Délégués à la Protection des Données
- Analyse de risques (ISO 27005)
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle… ;
- Expertises de systèmes de vote électronique ;

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

ou suivez nous sur

Réagissez à cet article

Source : *Europe : la Police pourrait prochainement consulter vos données personnelles sur Facebook sans autorisation*

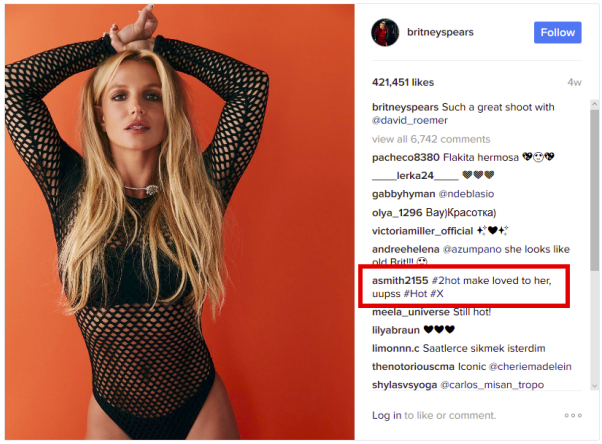
Instagram détourné pour espionner des membres de gouvernements

Instagram détourné pour espionner des membres de gouvernements

---

Turla, le groupe de cyberespionnage qui cible des représentants de gouvernements et des diplomates, lance une nouvelle attaque en se servant d'Instagram®. En février 2017, Forcepoint® a publié une liste de sites Internet récemment compromis.

Les cybercriminels utilisent **la technique d'attaque de trou d'eau**, qui vise à rediriger les victimes ayant cliqué sur un site compromis vers leurs serveurs C&C. Les chercheurs ESET® ont repéré **une extension de Firefox® qui utilise une URL bit.ly pour renvoyer vers les serveurs C&C. Le chemin de l'URL est diffusé via des commentaires d'une publication Instagram.** Dans l'échantillon analysé par ESET, l'un des commentaires s'affiche sur une photo du compte officiel de Britney Spears.



© https://www.instagram.com/p/BO8gU41A45g/

Pour obtenir l'URL bit.ly, l'extension scrute les commentaires de chaque photo et pour chaque commentaire en calcule un hash. Si la valeur de hash correspond à un code de déclenchement, l'extension exécute une opération pour convertir le commentaire en URL.

« L'utilisation par Turla des réseaux sociaux pour récupérer les adresses C&C ne facilite pas la tâche aux chercheurs en cybersécurité. Il est difficile de distinguer le trafic malveillant du trafic légitime sur les réseaux sociaux, » explique Jean-Ian Boutin, Senior Malware Researcher chez ESET. Par ailleurs, c**ette technique offre plus de souplesse aux pirates :** « comme l'information nécessaire pour obtenir l'URL du serveur C&C n'est autre qu'un commentaire sur les réseaux sociaux, **le cybercriminel a la possibilité de le modifier ou de l'effacer** à tout moment, » poursuit Jean-Ian Boutin.

Pour éviter d'être infecté par une attaque de trou d'eau de ce type, les chercheurs ESET recommandent de :

- mettre à jour les navigateurs et les plugins des navigateurs
- éviter de télécharger ou d'installer des extensions venant de sources non vérifiées
- utiliser une solution de sécurité (à jour) capable de détecter les sites Internet compromis

Seuls 17 clics ont été enregistrés sur ce lien en février lorsque le commentaire a été posté. Le nombre étant relativement faible, ESET suppose qu'il s'agit d'un test pour une attaque de plus grande envergure.

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

---

Réagissez à cet article

Source : *ESET*

Mettez à jour votre téléphone sous Android. 101 failles dont 27 critiques à corriger

Mettez à jour votre téléphone sous Android. 101 failles dont 27 critiques à corriger

Plus d'une centaine de vulnérabilités sont retirées d'Android. Dont de nombreuses liées aux puces de l'américain Qualcomm.

Google vient de publier le bulletin de sécurité de juin concernant le système d'exploitation mobile **Android** (en moutures 4.4, 5.0, 5.1, 6.0, 7.0 et 7.1).
Au menu, la correction de **101** failles de sécurité, dont **27** sont considérées comme critiques. Ces dernières permettent potentiellement la prise de contrôle du téléphone par une application malveillante.
La plupart de ces failles critiques touchent le code livré par **Qualcomm** pour ses puces. Le concepteur américain de SoC ARM montre ici sa capacité à proposer un bon « service après-vente » logiciel. Avec une amélioration constante des pilotes et applicatifs liés à ses offres.

Mise à jour au bon vouloir des constructeurs

Bien évidemment, il est vivement conseillé d'installer cette mise à jour d'Android rapidement. À condition bien entendu que votre constructeur de smartphone la relaie. Pas de souci à attendre du côté des terminaux mobiles distribués par Google. Les **Nexus** 5X, 6, 6P, 9, Player, ainsi que les **Pixel**, C et XL ont en effet déjà eu droit à cet update…[lire la suite]

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

---

Réagissez à cet article

Source : *Google corrige 101 failles d'Android, dont 27 critiques*

Over 8,600 Vulnerabilities Found in Pacemakers

Over 8,600 Vulnerabilities Found in Pacemakers

Millions of people that rely on pacemakers to keep their hearts beating are at risk of software glitches and hackers, which could eventually take their lives. A pacemaker is a small electrical battery-operated device that's surgically implanted in the chest to help control the heartbeats.…[Lire la suite]

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 de formation, de sensibilisation ou d'audits 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 sur cette page.

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

Alerte : Mettez à jour votre Google Chrome

Alerte : Mettez à jour votre Google Chrome

Sur Windows, MacOs et Linux, de multiples vulnérabilités dans Google Chrome ont été détectées par le CERT (Computer Emergency Reponse Team) de l'ANSSI (Agence nationale de la sécurité des systèmes d'information).

Systèmes affectés

Chrome versions antérieures à 59.0.3071.86 pour Windows, Mac et Linux

Résumé

De multiples vulnérabilités ont été corrigées dans Google Chrome. Elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur et un contournement de la politique de sécurité.

Comment mettre à jour ?

Cliquez sur les 3 points verticaux (en haut à droite du navigateur), descendez la souris sur « Aide » et cliquez sur « À propos de Google Chrome » et sur « Mise à jour ».
Sinon, vous pouvez aussi télécharger la dernière version de Google Chrome sur « https://www.google.fr/chrome/browser/desktop/index.html »
[Plus d'infos ici]

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

---

Réagissez à cet article

Source : *Multiples vulnérabilités dans Google Chrome*

Mettez à jour de toute urgence votre Windows

	Mettez à jour de toute urgence votre Windows

Une vulnérabilité critique découverte par Google et touchant Windows a vite été corrigée par Microsoft. Au bénéfice de ceux qui laissent Windows Update activé.

La semaine dernière, le 24 mai, Microsoft a discrètement corrigé une vulnérabilité critique du composant MsMpEng de Windows. Plus précisément, MsMpEng est un processus de base de Windows Defender, le logiciel anti-malware livré en standard sur Windows 10 et 8.1, et installable sur Windows 7. Découverte le 12 mai dernier par Tavis Ormandy, chercheur en sécurité du Google Zero Project, cette faille autorise l'exécution de programmes non certifiés et donc potentiellement malveillants.
« MsMpEng comprend un émulateur système x86 complet qui est utilisé pour exécuter des fichiers non fiables qui ressemblent à des programmes exécutables. L'émulateur s'exécute sous la forme NT AUTHORITY\SYSTEM et ne réside pas dans un bac à sable », explique l'expert sur la page signalant le bug. Et sur laquelle il revient avec moult détails techniques sur le mode d'exploitation de la vulnérabilité.
Cette nouvelle brèche qui touche l'anti-malware de Microsoft est la deuxième que Tavis Ormandy déniche à quelques jours d'intervalle. Le 9 mai dernier, une faille de MsMpEng risquait d'infecter les utilisateurs… qui lançaient une inspection de leur machine à l'aide de l'outil de sécurité. Paradoxalement, les utilisateurs qui avaient désactivé le scan automatique en étaient donc protégés…[lire la suite]

Denis JACOPINI :
Vous avez aussi la possibilité (et nous vous recommandons fortement) d'installer un logiciel de sécurité géré par ceux pour qui la cybersécurité est le métier. Nous vous recommandons depuis 1996 les produits ESET et en particulier celui-ci (cliquez).

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 ;
  (Autorisation de la DRTEF n°93 84 03041 84)
- 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 : *Microsoft corrige encore Windows Defender en toute discrétion*

Microsoft corrige encore Windows Defender en toute discrétion

Mettez à jour de toute urgence votre Windows

Une vulnérabilité critique découverte par Google et touchant Windows a vite été corrigée par Microsoft. Au bénéfice de ceux qui laissent Windows Update activé.

La semaine dernière, le 24 mai, Microsoft a discrètement corrigé une vulnérabilité critique du composant MsMpEng de Windows. Plus précisément, MsMpEng est un processus de base de Windows Defender, le logiciel anti-malware livré en standard sur Windows 10 et 8.1, et installable sur Windows 7. Découverte le 12 mai dernier par Tavis Ormandy, chercheur en sécurité du Google Zero Project, cette faille autorise l'exécution de programmes non certifiés et donc potentiellement malveillants.
« MsMpEng comprend un émulateur système x86 complet qui est utilisé pour exécuter des fichiers non fiables qui ressemblent à des programmes exécutables. L'émulateur s'exécute sous la forme NT AUTHORITY\SYSTEM et ne réside pas dans un bac à sable », explique l'expert sur la page signalant le bug. Et sur laquelle il revient avec moult détails techniques sur le mode d'exploitation de la vulnérabilité.
Cette nouvelle brèche qui touche l'anti-malware de Microsoft est la deuxième que Tavis Ormandy déniche à quelques jours d'intervalle. Le 9 mai dernier, une faille de MsMpEng risquait d'infecter les utilisateurs… qui lançaient une inspection de leur machine à l'aide de l'outil de sécurité. Paradoxalement, les utilisateurs qui avaient désactivé le scan automatique en étaient donc protégés…[lire la suite]

Denis JACOPINI :
Vous avez aussi la possibilité (et nous vous recommandons fortement) d'installer un logiciel de sécurité géré par ceux pour qui la cybersécurité est le métier. Nous vous recommandons depuis 1996 les produits ESET et en particulier celui-ci (cliquez).

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 ;
  (Autorisation de la DRTEF n°93 84 03041 84)
- 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 : *Microsoft corrige encore Windows Defender en toute discrétion*

Judy Android Malware Infects Over 36.5 Million Google Play Store Users

Judy Android Malware Infects Over 36.5 Million Google Play Store Users

---

Security researchers have claimed to have discovered possibly the largest malware campaign on Google Play Store that has already infected around 36.5 million Android devices with malicious ad-click software.

The security firm Checkpoint on Thursday published a blog post revealing more than 41 Android applications from a Korean company on Google Play Store that make money for its creators by creating fake advertisement clicks from the infected devices.

All the malicious apps, developed by Korea-based Kiniwini and published under the moniker ENISTUDIO Corp, contained an adware program, dubbed Judy, that is being used to generate fraudulent clicks to generate revenue from advertisements.

Moreover, the researchers also uncovered a few more apps, published by other developers on Play Store, inexplicably containing the same the malware in them…[lire la suite]

Réagissez à cet article

Source : *Judy Android Malware Infects Over 36.5 Million Google Play Store Users*

Un simple lien permet de faire planter les PC Windows 7 et 8.1

Un simple lien permet de faire planter les PC Windows 7 et 8.1

Un bug du NTFS exploitable depuis le web met à genoux les PC Windows. Windows 10 est épargné, mais Windows 7 et 8.1 devront être corrigés.
À l'époque de Windows 95 et Windows 98, un bug permettait de faire planter un PC via un simple document au nom non supporté par le système de fichiers. Il suffisait pour cela d'accéder à certains périphériques, représentés par un nom de fichier virtuel.
Aussi incroyable que cela paraisse, un bug similaire existe dans **Windows 7 et Windows 8.1**, dévoile *Ars Technica*. Tenter d'accéder au fichier « **c:\$MFT\123** » bloque complètement le système de fichiers NTFS. La MFT n'est pas en principe accessible directement, mais en la traitant comme un dossier, son accès est totalement bloqué. Tout le système se trouve alors figé, ne pouvant plus accéder aux données de la partition NTFS concernée. Seule solution : redémarrer la machine…[lire la suite]

Réagissez à cet article

Source : *Un simple lien permet de faire planter les PC Windows 7 et 8.1*

Mieux protéger les TPE/PME du cyber-risque

	Mieux protéger les TPE/PME du cyber-risque

Les cyberattaques concernent tous les acteurs de la société: particuliers, entreprises ou administrations. Mais force est de constater que les principaux impactés sont généralement les entreprises de petite ou de moyenne taille.
Une étude IFOP montre que, en France, près de **77% des cyberattaques toucheraient les TPE/PME**. Par ailleurs, les dommages de ces attaques numériques peuvent se révéler d'une importance telle qu'elle pourrait compromettre l'avenir même de l'entité touchée. Outre la **baisse ou l'interruption des activités** pendant une certaine durée, une cyberattaque peut également **impacter la réputation ainsi que les relations contractuelles** de l'entreprise touchée, notamment celles avec ses partenaires et/ou sa clientèle.
Pourtant, seulement **un tiers des entreprises de petite ou moyenne taille se dit consciente des dangers d'une cyberattaque** et prend les précautions de prévention nécessaires. Pour les autres, elles disposeraient de systèmes vulnérables et facilement accessibles aux hackeurs.

Les assureurs : nouveaux acteurs de la cybersécurité

Si la plupart des assureurs proposent désormais aux professionnels des **assurances cyber-risques** et **e-reputation,** un assureur a décidé d'aller plus loin. Generali s'associe à ENGIE Ineo et Europ Assistance pour lancer une **offre d'assurance spécifique pour les TPE/PME**. Cette dernière vise la réparation et l'indemnisation de ces entreprises en cas de cyberattaque. Le partenariat entre les trois sociétés a pour but d'optimiser au maximum la prise en charge de l'entreprise touchée. Elle sera axée sur trois points :

•

Europ Assistance assurera une prise en charge immédiate :

Europ Assistance dispose d'un **service d'assistance informatique disponible à tout moment**. Elle prendra en charge l'entreprise victime d'une cyberattaque dans les plus brefs délais. Les chargés d'assistance travailleront en collaboration avec les experts informatiques d'Engie Ineo. Ils mettent également en place un accompagnement humain de l'entreprise afin de s'assurer qu'elle comprenne les différentes étapes du processus de restauration.

•

La réparation des données par Engie Ineo

Une fois la cyberattaque avérée, la société Engie Ineo sera chargée de **restaurer les données informatiques**. A cet effet, son équipe technique devra effectuer une enquête pour établir un diagnostic et déceler les preuves de l'attaque. Ils doivent ensuite reconstituer et restaurer les différentes données volées ou cryptées par les hackeurs. Le contrat d'assurance prévoit une **garantie « temps d'intervention » d'une heure.** Enfin, les services informatiques de l'entreprise devront étroitement collaborer avec la société Engie Ineo.

•

Generali indemnisera les dommages

Pour l'assureur Generali, sa mission tiendra à l'**indemnisation des dommages matériels mais aussi des pertes financières** découlant de l'attaque. Elle prendra donc en charge les frais d'expertise et de restauration des données, les pertes d'exploitation ainsi que la responsabilité civile et autres frais générés par la cyberattaque.Pour couvrir exactement chaque entreprise assurée, Generali prévoit de mettre en place un questionnaire spécifique afin d'évaluer le niveau d'exposition de l'entreprise au risque d'attaque numérique et d'adapter la protection selon sa taille.

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 ;
  (Autorisation de la DRTEF n°93 84 03041 84)
- 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 : *Cyberattaques: l'assurance se développe*