Comment se préparer aux incidents de sécurité ?

	Comment se préparer aux incidents de sécurité ?

Les entreprises doivent être prêtes à agir face à des incidents de sécurité et à des attaques. Et cela passe notamment par sept points précis (par Peter Sullivan).

Un plan de préparation à la cybersécurité présente et détaille les objectifs fondamentaux que l'organisation doit atteindre pour se considérer comme prête à faire face à des incidents de sécurité informatique. La liste de contrôles qui va suivre n'est pas exhaustive, mais elle souligne des objectifs qui constituent un minimum requis pour donner un niveau raisonnable de sensibilisation à la cybersécurité et se concentrer sur la protection des actifs informationnels essentiels.
Ici, la préparation à la cybersécurité est définie comme l'état permettant de détecter et de réagir efficacement aux brèches et aux intrusions informatiques, aux attaques de logiciels malveillants, aux attaques par hameçonnage, au vol de données et aux atteintes à la propriété intellectuelle – tant à l'extérieur qu'à l'intérieur du réseau.
Un élément essentiel de cette définition est de « pouvoir détecter ». La détection est un domaine où une amélioration significative peut être atteinte en abaissant le délai de détection, couramment observé entre 9 et 18 mois. Une capacité de détection plus rapide permet de limiter les dommages causés par une intrusion et de réduire le coût de récupération de cette intrusion. Être capable de comprendre les activités régulières du réseau et de détecter ce qui diverge de la norme est un élément important de la préparation à la cybersécurité. Voici une sept objectifs que les entreprises devraient considérer.

Les objectifs à atteindre

1. Plan de cybersécurité
2. Gestion du risque
3. Gestion de l'identité
- **Contrôle d'accès**
- **Authentification**
- **Autorisation**
- **Responsabilité**

4. Surveillance de réseau
5. Architecture de sécurité
6. Contrôle des actifs, des configurations et des changements
7. Cartographie de la gestion des incidents
…[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 : *Se préparer aux incidents de sécurité*

Vous êtes le maillon faible (en cybersécurité)

	Vous êtes le maillon faible (en cybersécurité)

Encore une fois, une étude pointe l'importance du facteur humain dans les problèmes de cybersécurité, cette fois réalisée par Kaspersky.

De HAL à Skynet, les ordinateurs n'ont-ils pas raison de vouloir éliminer les humains ? Les études pointant le facteur humain comme maillon faible de la cybersécurité se multiplient en effet. Celle qui vient d'être publiée par l'éditeur Kaspersky s'ajoute à la longue liste en pointant les principales causes d'incidents et les mauvaises pratiques.

Parmi les plus mauvaises pratiques, la dissimulation des incidents de cybersécurité est adoptée dans 40 % des entreprises. Or la dissimulation empêche la correction. Et 46 % des incidents sont eux-mêmes issus d'actions de collaborateurs internes. En présence d'un malware, un incident sera déclenché dans 53 % des cas par une action inappropriée d'un collaborateur.

Les attaques ciblées utilisent souvent les collaborateurs comme portes d'entrée

Les attaques ciblées restent dominées par l'action d'un tel malware (49 % des cas). L'exploitation des failles techniques ou des fuites via des terminaux mobiles représente 30 % Et l'ingénierie sociale (hameçonnage inclus) est la troisième cause d'infection avec 28 % des cas.

Les mauvaises pratiques sont nombreuses. Tomber dans le piège d'un phishing n'est qu'un des cas. Il y a aussi les mots de passe trop faibles, les faux appels du support technique, les clés USB abandonnées dans un parking qui sont systématiquement récupérées… Et la dissimulation d'incident est probablement le pire.

Source : cio-online.com *Vous êtes le maillon faible (en cybersécurité)*

NOTRE MÉTIER :

EXPERTISES / COLLECTE & RECHERCHE DE PREUVES : Nous mettons à votre disposition notre expérience en matière d'expertise technique et judiciaire ainsi que nos meilleurs équipements en vue de collecter ou rechercher des preuves dans des téléphones, ordinateurs et autres équipements numériques;

PRÉVENTION : Nous vous apprenons à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) sous forme de conférences, d'audits ou de formations ;

SUPERVISION : En collaboration avec votre société de maintenance informatique, nous assurons le suivi de la sécurité de votre installation pour son efficience maximale ;

AUDITS CNIL / AUDIT SÉCURITÉ / ANALYSE D'IMPACT : Fort de notre expérience d'une vingtaine d'années, de notre certification en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005) et des formations suivies auprès de la CNIL, nous réaliseront un état des lieux (audit) de votre installation en vue de son amélioration, d'une analyse d'impact ou de sa mise en conformité ;

MISE EN CONFORMITÉ CNIL/RGPD : Nous mettons à niveau une personne de votre établissement qui deviendra référent CNIL et nous l'assistons dans vos démarches de mise en conformité avec le RGPD (Réglement Européen relatif à la Protection des Données à caractère personnel).

Besoin d'un Expert ? contactez-vous

NOS FORMATIONS

: https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles (Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle)

Réagissez à cet article

Source : *Vous êtes le maillon faible (en cybersécurité)*

Comment a évolué la cybercriminalité en 2016 par rapport à 2015 ?

	Comment a évolué la cybercriminalité en 2016 par rapport à 2015 ?

Il y a les cyberattaques à l'échelle des états et il y a la cybercriminalité qui peut toucher chaque citoyen. Vols de mots de passe, demandes de rançon, vols de données personnelles… Les chiffres sont en hausse partout dans le monde mais aussi en France.

Les chiffres de la cybercriminalité ont de quoi faire peur. 13,7 millions de personnes ont été confrontées à la cybercriminalité en France en 2016, selon Norton, entreprise spécialisée dans la sécurité en ligne.
Vente de faux papiers d'identité, apologie du terrorisme, vols de mots de passe, de données personnelles, extorsion de fonds ou encore trafic d'armes : le terme cybercriminalité couvre de multiples activités illicites.

Selon Symantec, célèbre pour ses logiciels antivirus, le nombre de cyberattaques dans le monde a diminué ces derniers mois. | Visactu

Vol de mots de passe

En France, les actes les plus fréquents sont les vols de mots de passe (14 % des cas) et la fraude à la carte bancaire (10 % des cas). Mais entre les faits recensés et la réalité, il est très difficile de mesurer l'ampleur exacte du phénomène…
Certaines victimes ne savent tout simplement pas (encore) qu'elles ont été volées, d'autres n'ont pas porté plainte et ont préféré payer une rançon (parfois quelques centaines d'euros) pour récupérer des photos intimes par exemple.
Selon Symantec, célèbre pour ses logiciels antivirus, le nombre de cyberattaques dans le monde a diminué ces derniers mois. Elle en a recensé 291 000 pour le seul mois de novembre 2016 contre 1 461 000 en janvier 2015.

Gare aux malwares

Par contre, le nombre de nouveaux malwares explose. Ces logiciels malveillants qui accèdent à l'appareil d'un utilisateur à son insu (logiciel espion, virus, cheval de Troie, rootkits, etc.) dans le but de dérober des données sont partout.
Symantec dénombrait 20 millions de nouveaux malwares (et variantes) chaque mois début 2016, un chiffre qui a bondi en fin d'année pour atteindre les 96,1 millions en novembre et 71,2 millions de nouveaux malwares détectés en décembre.

Les vols de données de personnelles en hausse

En novembre 2016, Symantec estimait qu'un email sur 85 contenait un malware, qu'un email sur 2 620 était une tentative de phishing (l'email vous invite à cliquer vers un faux site afin de voler vos identifiants, mots de passe, etc.) et que plus de la moitié des emails (54,3 %) étaient non sollicités (spam).
En 2015, elle estimait que 429 millions de personnes dans le monde s'étaient faites voler des données personnelles, un chiffre en hausse de 23 % par rapport à l'année précédente.

Original de l'article : La cybercriminalité en hausse en France et dans le monde

---

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 : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Original de l’article mis en page : La cybercriminalité en hausse en France et dans le monde

---

Vigilance – faux appels passés au nom de la CNIL

Vigilance – faux appels passés au nom de la CNIL

Vigilance – faux appels passés au nom de la CNIL

Des entreprises ont reçu, ces derniers jours, des appels téléphoniques de personnes se faisant passer pour la CNIL et prétextant devoir envoyer des documents.
Ces appels frauduleux ont pour but de collecter des informations sur votre organisation, et notamment l’adresse mail de dirigeants (directeur informatique, directeur des achats, etc.), pour préparer une attaque informatique (rançongiciel / ransomware) ou une escroquerie financière (« arnaque au Président »).
N’y répondez pas ! En cas de doute, vous pouvez contacter la CNIL au 01 53 73 22 22

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 : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Original de l’article mis en page : Vigilance – faux appels passés au nom de la CNIL | CNIL

Prévisions cybercriminalité pour 2017

	Prévisions cybercriminalité pour 2017

Nous sommes tombés sur cet article sur le site Internet « Informaticien.be » et n'avons pas pu nous empêcher de le partager avec vous tant il est en accord avec les prévisions ressorties de nos analyses. Aux portes de 2017, les entreprises, administrations et association non seulement vont devoir s'adapter à une réglementation Européenne risquant s'impacter lourdement la réputation des établissements qui devront signaler à la CNIL qu'elle viennent d'être victime de piratage, mais également, l'évolution des techniques de piratage vont augmenter les risques qu'auront les organismes à se faire pirater leurs systèmes informatiques. N'hésitez pas à consulter notre page consacrée aux bons conseils que nous prodiguons depuis de nombreuses années sur https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles.
Denis JACOPINI

Trend Micro présente son rapport annuel des prévisions en matière de sécurité: 'The Next Tier – 8 Security Predictions for 2017'. L'année prochaine sera marquée par des attaques de plus grande envergure à tous les niveaux. Les cybercriminels adopteront des tactiques différentes pour tirer parti de l'évolution du paysage technologique.
« Nous pensons que la General Data Protection Regulation (GDPR) va non seulement changer fondamentalement la manière dont les entreprises gèrent leurs données, mais aussi induire de nouvelles méthodes d'attaque. La tactique du ransomware va également s'étendre pour toucher plus d'appareils, tandis que la cyberpropagande influencera de plus en plus l'opinion publique", déclare Raimund Genes, CTO de Trend Micro.
En 2016, l'on a assisté à une formidable augmentation des vulnérabilités d'Apple avec pas moins de 50 fuites. A cela s'ajoutent 135 bugs Adobe et 76 bugs Microsoft. Alors que Microsoft continue d'améliorer ses facteurs limitatifs et qu'Apple est de plus en plus considéré comme le système d'exploitation prépondérant, ce déplacement apparent des 'exploits' des logiciels vulnérables va encore s'accentuer en 2017.
L'IoT et l'IIoT – dans la ligne de mire des attaques ciblées
L'Internet of Things (IoT – internet des objets) et l'Industrial Internet of Things (IioT – internet industriel des objets) seront de plus en plus dans la ligne de mire des attaques ciblées en 2017. Ces attaques tirent parti de l'engouement croissant suscité par les appareils connectés en exploitant les failles et les systèmes non protégés et en perturbant des processus d'entreprise. L'usage croissant d'appareils mobiles pour surveiller les systèmes de production dans les usines et les milieux industriels, combiné au nombre important de vulnérabilités dans ces systèmes constitue une réelle menace pour les organisations.
Explosion de l'extorsion professionnelle
Le Business E-mail Compromise (BEC) et le Business Process Compromise (BPC) représentent de plus en plus une forme relativement simple et économiquement rentable d'extorsion professionnelle. En incitant un employé innocent à verser de l'argent sur le compte bancaire d'un criminel, une attaque BEC peut rapporter 140.000 dollars. Bien que le piratage direct d'un système de transaction financière exige plus d'efforts, cela représente une manne de pas moins de 81 millions de dollars pouvant tomber aux mains des criminels.
Autres faits marquants du rapport
Le nombre de nouvelles familles de ransomware ne progresse que de 25 %. Mais le ransomware s'étend désormais aux appareils IoT et aux terminaux informatiques autres que les desktops (par exemple les systèmes POS ou les distributeurs automatiques).
Les fournisseurs ne parviendront pas à protéger à temps les appareils IoT et IIoT pour éviter des attaques DoS (refus de service) ou d'autres types d'attaques.
Le nombre de failles découvertes dans les technologies Apple et Adobe augmente, ce qui vient s'ajouter aux « exploit-kits ».
46 pour cent de la population mondiale est aujourd'hui reliée à l'internet : la cyberpropagande ne va cesser d'augmenter, à présent que les nouveaux dirigeants des grands pays sont en place. L'opinion publique risque donc d'être influencée par de fausses informations.
Comme ce fut le cas lors de l'attaque de la Banque du Bangladesh plus tôt cette année, les cybercriminels parviennent à modifier des processus d'entreprise via des attaques BPC, et à en tirer largement profit. Les attaques BEC restent d'actualité pour extorquer des fonds à des employés qui ne se doutent de rien.
Le GDPR produira des changements de politique et administratifs qui auront un lourd impact sur les coûts. Cela exigera aussi des examens complexes des processus de données pour assurer la conformité réglementaire.
De nouvelles méthodes d'attaques ciblées déjoueront les techniques de détection modernes, permettant aux criminels de s'attaquer à différentes organisations.
Original de l'article mis en page : Le ransomware s'étend aux appareils connectés et à l'internet des objets – Press Releases – Informaticien.be

---

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 : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Original de l’article mis en page : Le ransomware s’étend aux appareils connectés et à l’internet des objets – Press Releases – Informaticien.be