Conseils clé pour se protéger contre la cybercriminalité | Denis JACOPINI

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

#Conseils clé pour #se protéger contre la #cybercriminalité

L’avis d’expert de Jean-Philippe Sanchez, Consultant Sécurité chez NetIQ France.

La cybercriminalité est souvent médiatisée lorsque d’énormes failles de sécurité sont révélées et que les dommages sont significatifs pour les entreprises touchées. L’attaque massive organisée par des pirates informatiques russes il y a quelques semaines à une échelle mondiale en est un très bel et marquant exemple, avec plus de 1,2 milliard de mots de passe volés.

Mais les hackers ne se limitent pas aux attaques massives, et des petites brèches de sécurité d’apparence anodines peuvent pourtant s’avérer avoir de lourdes conséquences, tant pour les grandes entreprises que pour les plus petites organisations possédant des données sensibles ou à forte valeur ajoutée.

Ne perdez pas votre temps à anticiper, sachez surtout détecter les failles et limiter les dégâts

La meilleure chose qu’un directeur informatique ou un responsable de la sécurité puisse faire pour protéger son entreprise est de comprendre et d’accepter l’impossibilité de maintenir les attaquants à l’écart. Tout le monde est tôt ou tard victime d’une faille de sécurité. Le plus important est de savoir dans quel délai vous la détecterez et dans quelle mesure vous pourrez limiter les dommages. Il convient de mettre l’accent sur la réduction du risque dans les domaines clés et la surveillance des événements au niveau du pare-feu pour détecter le plus rapidement possible l’intrusion d’un attaquant et la tentative de vol de données. Toute autre action ne reviendra qu’à reproduire des stratégies qui ont déjà montré leurs limites dans le passé, pour un coût encore plus élevé.

Axez votre stratégie de sécurité sur l’identité et les données, et non plus l’infrastructure

Le mode de pensée centré sur le réseau et les appareils est de plus en plus délaissé en faveur d’une sécurité axée sur l’identité et les données.

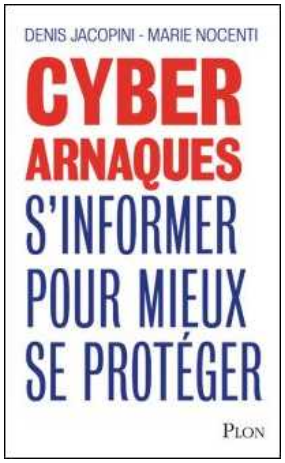
Désormais, tenter de protéger l’infrastructure de l’entreprise n’apparaît plus comme une solution gagnante. Avec l’usage croissant de l’informatique mobile et du Cloud computing, cette tâche s’avère souvent trop complexe et n’est plus entièrement maîtrisée par le personnel informatique et de sécurité. En revanche, le personnel chargé de la sécurité réfléchit de plus en plus à la protection des données transférées d’un endroit à un autre, y compris dans le cloud, et à l’acquisition d’une meilleure connaissance de l’identité des individus qui ont accès à ces données. Néanmoins, suis-je certain de savoir qui accède actuellement à notre base de données de patients ? Est-il normal que ce salarié ouvre ce fichier de données clients ? Ces décisions sont de plus en plus complétées par l’introduction d’un contexte du type : dois-je permettre à ce salarié d’accéder à ces données sensibles alors qu’il est en vacances dans le Sud et qu’il se connecte depuis sa tablette dans un cybercafé ? Il s’agit là d’une façon plus intelligente (et efficace) d’appréhender les risques du comportement surveillé, en répondant aux problèmes de sécurité fondamentaux liés aux utilisateurs privilégiés, aux attaques internes et aux menaces persistantes avancées.

Ne misez pas tout sur la technologie, sensibilisez vos collaborateurs car ils sont les véhicules de vos données !

Il est toujours possible d’améliorer l’éducation – bien que je sois convaincu qu’il faille en changer le ton pour passer du « ne faites pas ceci » au « comme vous le ferez de toute façon, voici comment procéder pour éviter de prendre des risques ». Le pouvoir dans le monde de l’informatique professionnelle a changé de mains : il n’est plus dévolu au service IT autoritaire et centralisé, avec le personnel qui lui est associé, mais relève désormais des dirigeants de l’entreprise et des responsables métiers. Aujourd’hui plus que jamais, l’utilisateur de l’entreprise décide lui-même de la technologie à employer et de la façon de procéder. Dans ce contexte, l’éducation doit être recentrée sur les conseils et le choix de solutions sûres pour cesser de s’apparenter à une liste d’actions à éviter, qui sera de toute façon rarement respectée.

Réagissez à cet article

CYBERARNAQUES - S'informer pour mieux se protéger (Le Livre)
Denis JACOPINI Marie Nocenti (Plon) ISBN : 2259264220



Denis Jacopini, expert judiciaire en informatique diplômé et spécialisé en cybercriminalité, raconte, décrypte et donne des parades contre toutes les cyberarnaques dont chacun peut être victime.

Il est témoin depuis plus de 20 ans d'attaques de sites Internet, de piratages d'ordinateurs, de dépouillements de comptes bancaires et d'autres arnaques toujours plus sournoisement élaborées.

Parce qu'il s'est rendu compte qu'à sa modeste échelle il ne pourrait sensibiliser tout le monde au travers des formations et des conférences qu'il anime en France et à l'étranger, il a imaginé cet ouvrage afin d'alerter tous ceux qui se posent la question : Et si ça m'arrivait un jour ?

Plutôt que de présenter une longue liste d'arnaques Internet recensées depuis plusieurs années, Denis Jacopini, avec la collaboration de Marie Nocenti, auteur du roman Le sourire d'un ange, a souhaité vous faire partager la vie de victimes d'arnaques Internet en se basant sur des faits réels, présentés sous forme de nouvelles suivies de recommandations pour s'en prémunir. Et si un jour vous rencontrez des circonstances similaires, vous aurez le réflexe de vous méfier sans risquer de vivre la fin tragique de ces histoires et d'en subir les conséquences parfois dramatiques.

Pour éviter de faire entrer le loup dans votre bergerie, il est essentiel de le connaître pour le reconnaître !

Commandez sur Fnac.fr

https://www.youtube.com/watch?v=lDw3kI7ra2s

06/04/2018 A l'occasion de la sortie de son livre "CYBERARNAQUES : S'informer pour mieux se protéger",Denis JACOPINI répond aux questions de Valérie BENHAÏM et ses 4 invités : 7 Millions de victimes de la Cybercriminalité en 2010 (Symantec) 13,8 Milions de victimes de la Cybercirminalité en 2016 (Symantec) 19,3 Millions de victimes de la Cybercriminalité en 2017 (Symantec) Plus ça va moins ça va ? Peut-on acheter sur Internet sans risque ? Si le site Internet est à l'étranger, il ne faut pas y aller ? Comment éviter de se faire arnaquer ? Comment on fait pour renifler une arnaque sur Internet ? Comment avoir un coup d'avance sur les pirates informatiques ? Quelle est l'arnaque qui revient le plus souvent ? Denis JACOPINI vous répond sur C8 avec Valérie BENHAÏM et ses invités.

Commandez sur Fnac.fr

---

https://youtu.be/usg12zkRD9I?list=UUoHqj_HKcbzRuvIPdu3FktA

12/04/2018 Denis JACOPINI est invité sur Europe 1 à l'occasion de la sortie du livre "CYBERARNAQUES S'informer pour mieux se protéger"
Comment se protéger des arnaques Internet

Commandez sur amazon.fr

Je me présente : Denis JACOPINI. Je suis l'auteur de ce livre coécrit avec Marie Nocenti, romancière.
Pour ma part, je suis Expert de justice en informatique spécialisé en cybercriminalité depuis 1996 et en protection des Données à Caractère Personnel.
J'anime des formations et des conférences sur le RGPD et la Cybercriminalité pour aider les organismes à se protéger des pirates informatiques et à se mettre en conformité avec la réglementation autour du numérique (dont le RGPD : Règlement Général sur la Protection des Données).

Commandez sur Fnac.fr

Source : http://www.generation-nt.com/cybercriminalite-hacker-netiq-jean-philippe-sanchez-actualite-1905811.html