Les failles utilisées par les hackers ont plus de 10 ans

	Les failles utilisées par les hackers ont plus de 10 ans

Les récentes attaques de malwares et de ransomwares survenues en 2017, dont WannaCry et Petya/NotPetya ont été les plus répandues et médiatisées, ont permis aux spécialistes de la cybersécurité d'avoir une vision plus claire des failles utilisées par les hackers.

Fortinet, spécialiste de la cybersécurité, a analysé les attaques dont ont été victimes ses clients, généralement des entreprises. Dans le rapport publié en août 2017, il est mis l'accent sur la vétusté des failles utilisées par les hackers : la très grande majorité des attaques n'aurait pas pu être menée à bien si les systèmes avaient été mis à jour.
Les chiffres sont éloquents : dans 90 % des cas, les victimes ont été attaquées par le biais de failles datant de plus de 3 ans et dans 60 % des cas, ces failles étaient vieilles de 10 ans voire plus. L'attaque WannaCry a utilisé la faille EternalBlue de Windows qui faisait partie des outils de la NSA pour espionner ses cibles. Cette faille avait été rendue publique par les hackers du groupe *The Shadow Brockers*…[lire la suite]

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)

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 : *Les failles utilisées par les hackers ont plus de 10 ans*