OUCH! | Mai, 2018

SANS SECURITY AWARENESS

La Newsletter mensuelle de Sensibilisation à la Sécurité destinée aux utilisateurs informatiques

RGPD

Vue d'ensemble

Les emails et les services de messagerie (tels que Skype, Twitter ou Snapchat) sont l'un des principaux moyens de communication. Nous utilisons non seulement ces technologies quotidiennement pour travailler mais aussi pour rester en contact avec nos amis et notre famille. En conséquence, beaucoup de personnes dans le monde dépendent de ces technologies, devenues l'une des principales méthodes d'attaque utilisées par les cyber-attaquants, une méthode d'attaque appelée phishing (ou hameçonnage). Apprenez ce qu'est le phishing et comment vous pouvez repérer et arrêter ces attaques, que vous soyez au travail ou à la maison.

Le phishing est un type d'attaque qui utilise le courrier électronique ou un service de messagerie pour vous tromper dans une action que vous ne devez pas entreprendre, par exemple cliquer sur un lien malveillant, partager votre mot de passe ou encore ouvrir une pièce jointe infectée. Les attaquants travaillent dur pour rendre ces messages convaincants et appuient sur vos déclencheurs émotionnels, tels que l'urgence ou la curiosité. Ces messages peuvent donner l'impression qu'ils proviennent de quelqu'un ou de quelque chose que vous connaissez, comme d'un ami ou d'une entreprise de confiance. Ils peuvent même ajouter les logos de votre banque ou falsifier l'adresse e-mail pour que le message apparaisse plus légitime. Les attaquants envoient ensuite ces messages à des millions de personnes. Ils ne savent pas qui prendra l'appât, tout ce qu'ils savent c'est que plus ils enverront de messages, plus les victimes seront nombreuses.

Les données personnelles des individus doivent être traitées légalement, équitablement et de manière transparente.

Les gens doivent être informés de ce qui est collecté et dans quel but.

Les données personnelles doivent être collectées à des fins spécifiques, explicites et légitimes. Elles ne doivent pas être utilisées pour d'autres raisons qui entrent en conflit avec ces objectifs.

Les données personnelles ne doivent être conservées et traitées que le temps nécessaire à cette fin au maximum.

Les données personnelles doivent être tenues à jour et exactes.

Les personnes ont le droit de recevoir une copie de leurs données ou peuvent demander que leurs données personnelles ne soient plus utilisées, ou dans certains cas, supprimées intégralement.

Les organisations doivent mettre en œuvre des mesures de sécurité appropriées pour protéger les données personnelles contre la destruction, la perte, l'altération ou la divulgation accidentelle ou illégale.

En outre, les organisations doivent veiller à ce que tout le personnel chargé des données personnelles soit correctement formé à la sécurisation et à la protection de ces données.

Les mesures de protection mises en place pour sécuriser les données personnelles doivent assurer un niveau de protection adapté à la nature sensible des données. Au fur et à mesure que le risque associé aux données augmente, l'effort et le coût des mesures visant à protéger les données devront l'être également. Ces mesures devraient être régulièrement examinées et mises à jour, le cas échéant. Des dossiers bien documentés sur les décisions et les mesures de confidentialité et de sécurité aident à démontrer la conformité aux exigences. En outre, les organisations sont légalement tenues d'utiliser des mesures, telles que des contrats et des contrôles préalables, pour protéger les données personnelles lors de leur transfert à des tiers externes ou en particulier à des parties extérieures à l'Union européenne. Enfin, dans le cas d'une violation de données personnelles, les organisations doivent signaler la violation dans les 72 heures après en avoir pris connaissance. L'incapacité des organisations à se conformer à la RGPD peut entraîner des amendes pouvant aller jusqu'à 4% de leurs revenus globaux, faisant de la RGPD l'une des réglementations mondiales les plus coûteuses financièrement au monde.

Version Française

La société Pélissier & Partners spécialiste en Intelligence économique a été fondée sur une expérience de plus de quinze ans dans le domaine de la recherche d'information et de la cybersécurité dédiées aux dirigeants d'entreprises suisses.

Editeur invité

Brian Honan *est le PDG de BH Consulting, une société indépendante de conseil en cybersécurité et protection des données basée à Dublin en Irlande. Brian a été conseiller spécial du Centre de cybercriminalité d'Europol (EC3), fondateur du premier CERT en Irlande et membre du comité consultatif de plusieurs sociétés de sécurité innovantes. Vous pouvez trouver Brian sur* www.linkedin.com/in/brianhonan ou Twitter @brianhonan.

Sources

Vue d'ensemble de la RGPD pour les individus et les organisations : http://gdprandyou.ie

Le règlement RGPD : https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016R0679

Traductions et archives OUCH ! : https://www.sans.org/u/D88

Comité de rédaction : Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley | Traduit par : Marilyn Combet

Pélissier&Partners
Explorateurs de connaissances