DROIT

TD1/Partie2 - Découvrir Le Droit Des Données Et Le RGPD… : Le Cas VosRêves

Mission n°2:

Règlement du 25 mai 2018

Selon le nouveau règlement du 25 mai 2018, toute entreprise se doit de tenir un registre des activités de traitement afin de pouvoir démontrer le respect du règlement. Ensuite, elle est contrainte de mettre en place un ''Délégué à la protection des données''. Elle doit également s'assurer de la protection des données dès leur conception. Le règlement informe toutefois l'obligation de notifier les failles de sécurité à l'autorité de contrôle et aux individus. Par la suite, il est question d'une obligation à réaliser des études d'impact et consultation préalable auprès de l'autorité de contrôle pour le traitement de données sensibles et le profilage. Ensuite, le règlement fait allusion au même titre d'une obligation concernant la mise en place de nouveaux mécanismes d'encadrement de transfert des données hors UE. Enfin, les entreprises sont contraintes de mettre en place des responsabilités solidaires.

Des nouvelles menaces pour les entreprises

De multiples nouvelles menacent viennent compromettre la sécurité des données des entreprises. D'abord, les mails frauduleux diffusant des informations en cas d'ouverture aussi connu sous le nom de "phishing" . Ensuite, il existe un danger d'envergure similaire à propos d'un mail de dernier rappel qui expose un logo usurpé de la CNIL. Le message présent dans le mail évoque un numéro de téléphone à appeler pour ensuite facturer la fausse mise en conformité au règlement européen. Toutefois, les SMS peuvent également provenir d'une source non fiable. Ils représentent une menace du même ordre que les mails sujet au phishing.
D'autres part, d'après le cas courant. Certains escrocs sont prêts à demander une rançon à des entreprises sous la menace du verrouillage de leurs données, il s'agit du ransomware. Cependant, ils peuvent toutefois les contraindre sous la menace de la diffusion en public de ces données, ce cas relève alors de rancomhack.
Enfin le formjacking constitue une des menaces les plus récentes consistant à récupérer des informations bancaires grâce à un site de E-Commerce tel qu'amazon ou cdiscount, les hackers profitent d'une faille de sécurité du code source pour injecter leur code malveillant. Elle va de paire avec le cryptojacking qui consiste en l'injection d'un code dans la machine d'un autre afin de miner des formes d'argent virtuelles.

Mission n°3:

Synthèse de formation

Les différents articles illustrent les différentes menaces liées à la cybercriminalité. En effet, aujourd'hui, plus de 8 entreprises sur 10 sont sujettes à des attaques informatiques. De plus, ces attaques concernent autant les grandes entreprises que les PME toutefois elles sont souvent sous-estimées par les entreprises (seulement 43% de PDG considérant la cybersécurité comme étant essentielle à leur entreprise). Ce danger est d'autant plus sérieux qu'il ne s'accroît au travers de nouvelles menaces de pointes telles que le formjacking ou le crypto jacking. Il est donc primordial de sensibiliser les employés afin qu'ils adoptent les bons réflexes pour lutter contre le vols de données. Il faut savoir que le premier facteur de vol de données réside dans le vol de mot de passe. En effet, environ 90 % des mots de passe sont vulnérables face au piratage. Ensuite, à noter que le principal moyen d'infiltration de virus se trouve être les périphériques amovibles. Il est fortement déconseillé de connecter le même périphérique sur une machine diverse puis une de l'entreprise pour éviter une propagation automatiquement sur tous nouveaux périphériques amovibles connectés si jamais l'appareil initial est infecté par des codes malveillants. En conséquence, il est recommandé de former les employés aux réflexes suivants :

- Protégez les salariés partout où ils travaillent. Avec le développement du travail mobile, appliquer des mesures de sécurité au seul matériel présent au bureau n'est plus suffisant
- Effectuer un rapport quant à la sécurité interne et communiquer largement (mails, réunions d'information, affichage dans les locaux).
- interdire les applications non répertoriées (bloquer par défaut les applications inconnues)
- Sensibilisez vos collaborateurs au fait qu'ils travaillent pour une entreprise dont les données et les informations ont beaucoup de valeur sur le marché noir de la cybercriminalité, par la communication et la formation
- Précisez les conséquences éventuelles d'une attaque : demande de rançon, vol de données sensibles, coût de récupération des systèmes…
- Enseignez aux utilisateurs à faire appel à l'équipe informatique pour signaler n'importe quel incident
- Réalisez des simulations d'attaques de phishing pour tester la réactivité de vos collaborateurs à ces types d'attaques.

- Formez votre personnel aux menaces informatiques, à l'aide de cas concrets, facilement applicables dans leur quotidien

Mission n°4:

La chaîne de blocs

Les articles ci-dessus nous permettent d'expliquer ce que la chaîne de blocs nous octroie à l'heure actuelle mais commençons par expliquer ce qu'est la chaîne de blocs. La chaîne de block (blockchain *en anglais*) est une technologie de transmission d'informations à échelle mondiale, celle-ci peut être représentée par une immense Base de Données partagée avec tous ces utilisateurs. De part son partage au travers de ces multiples utilisateurs cela la rend bien plus efficace et sécurisé que d'autre moyen de stockage traditionnel. En effet, elle ressemble davantage à l'utilisation de monnaie virtuelle (*Ethereum, Bitcoin, …*), elle permet également de sécuriser et d'accélérer la plupart des transactions financières, mais aussi d'authentifier des documents officiels et de les archiver. Compte tenu de tous ces avantages, la blockchain semble parfaitement convenir à l'entreprise de M. Latour même si le travail à faire est fastidieux.

Bibliographie:

Sensibilisation à la sécurité informatique:

- Livre-blanc-sensibilisation-a-la-securite-informatique.pdf (kaspersky.com)

Application, le 25 mai 2018:

- Application, le 25 mai 2018, d'un nouveau règlement européen pour renforcer les droits et la protection des données personnelles (sne.fr)

PIERRE Geoffrey / MILLAN Romain