Fiche pratique n° 9 – Mesures de sécurité, techniques et organisationnelles (art 32)

Les responsabilités du responsable du traitement

L'organisation qui est le responsable du traitement doit mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque. Y sont inclus des moyens qui peuvent garantir la confidentialité, l'intégrité et la disponibilité des systèmes informatiques en place. Il doit également implémenter des moyens permettant de rétablir la disponibilité des données personnelles en cas d'incident (article 32 du RGPD).

En cas d'une violation de données personnelles, le responsable du traitement est tenu par l'article 33 du RGPD d'en notifier la CNPD. Le formulaire de notification d'une violation de données peut être téléchargé sur ce site de la CNPD et transmis à l'adresse email databreach@cnpd.lu.

Comment empêcher la réussite d'une attaque ?

Illustration des mesures techniques et organisationnelles à mettre en place pour réduire le risque de ransomware:

- **Sensibiliser les utilisateurs**: L'erreur humaine demeure un facteur majeur dans les violations de données. Le plus souvent, l'attaque par ransomware commence par l'ouverture d'une pièce jointe piégée ou la consultation d'une page web malveillante. Ainsi la formation des utilisateurs aux bonnes pratiques de sécurité numérique est une étape fondamentale pour lutter contre cette menace. L'objectif est également de faire naître ou de renforcer certains réflexes chez les utilisateurs en les invitant à signaler au service informatique de l'organisation tout élément suspect (exemple : pièce jointe ou courriel douteux, clé USB offerte, requêtes inhabituelles, etc.)

- **Créer un point de contact dédié**: Dédiez une ou plusieurs personnes que les utilisateurs du système informatique ont l'obligation de notifier en cas de suspicion d'un incident de sécurité. Ce point de contact doit être joignable à tout moment et chaque utilisateur doit savoir comment le contacter.

- **Exiger des mots de passe forts et uniques**: Tous les comptes d'utilisateur doivent être protégés par des mots de passe forts et uniques. L'authentification à deux facteurs (2FA) est aussi recommandée, surtout pour les accès depuis l'extérieur ainsi que pour les accès aux machines critiques de l'environnement informatique (p. ex. contrôleurs de domaine).

- **Sauvegarder les données**: Des sauvegardes régulières de l'ensemble des données, y compris celles présentes sur les serveurs de fichiers, d'infrastructure et d'applications métiers critiques doivent être réalisées. Ces sauvegardes, au moins pour les plus critiques, doivent être déconnectées du système d'information pour prévenir leur chiffrement, à l'instar des autres fichiers. L'usage de solutions de stockage à froid, comme des disques durs externes ou des bandes magnétiques, permet de protéger les sauvegardes d'une infection des systèmes et de conserver les données critiques à la reprise d'activité. La restauration d'un système informatique depuis des sauvegardes est un processus très complexe qui nécessite de la préparation et du temps. Il est utile de faire des tests et des simulations de restauration de façon régulière. Si, pour stocker des données à caractère personnel, vous utilisez un service d'informatique « cloud » dont les serveurs sont situés hors de l'Union européenne (UE) et de l'Espace Economique Européen (EEE), des exigences particulières

s’appliquent afin d’assurer un niveau de protection des données suffisant et approprié (voir aussi "Les transferts internationaux des données personnelles").

- **Maintenez à jour les logiciels et les systèmes**: Les vulnérabilités non corrigées des systèmes d’exploitation ou des logiciels présents sur le système d’information peuvent être utilisées pour infecter le système ou favoriser la propagation de l’infection. Il est crucial d’installer les mises à jour disponibles (incluant des correctifs de sécurité) dans les meilleurs délais. En outre, il est judicieux de désactiver les macros des solutions de bureautique qui permettent d’effectuer des tâches de manière automatisée afin d’éviter la propagation des ransomwares via les vulnérabilités de ces applications.
- **Utilisez et maintenez à jour les logiciels antivirus**: Bien que les antivirus ne garantissent pas de protection contre des ransomwares encore inconnus, l’utilisation de ces outils reste nécessaire sur les ressources exposées (postes de travail, serveurs de fichier, etc.). Pour que ces outils soient efficaces, il est important d’effectuer des mises à jour fréquentes et de s’assurer régulièrement de l’absence de logiciel malveillant connu sur les espaces de stockage des fichiers de l’entité.
- **Cloisonner le système d’information**: Sans mesure de protection et à partir d’une seule machine infectée, le ransomware peut se propager sur l’ensemble de votre système d’information et infecter la plupart des machines accessibles. Pour limiter le risque de propagation, il convient de segmenter le système d’information selon des zones présentant chacune un niveau de sécurité homogène (exemple : zone des serveurs internes, zone des serveurs exposés sur l’internet, zone des postes de travail utilisateurs, zone d’administration, etc.).
- **Limitez les droits des utilisateurs et les autorisations des applications**: Les utilisateurs ne doivent pas être administrateurs de leur poste de travail. Ceci limite la possibilité d’installation de logiciels et l’exécution involontaire de codes malveillants. Une autre bonne pratique consiste à limiter le nombre de comptes administrateurs et le nombre d’objets (utilisateurs, services, bibliothèques, applications, etc.) présents sur le système au strict nécessaire. En outre une revue régulière de ces utilisateurs et de leurs droits doit être effectuée dans le but de s’assurer que cela correspond à la réalité des besoins de l’organisation (départs d’employés, changements de postes, etc.).
- **Mettre en place un logiciel de chiffrement**: La mise en œuvre de technologies de cryptage représente une mesure de sécurité supplémentaire pour protéger vos données stockées. De ce fait, même si les criminels réussissent à voler vos données, ils n’arriveront pas à les accéder ni à les divulguer (sous réserve que les clés de chiffrement/déchiffrement ne soient pas compromises). Un mécanisme qui détecte l’altération massive des fichiers (en particulier par chiffrement) signale et limite les tentatives de cryptage de données exécutées par le ransomware. Une autre bonne pratique consiste à limiter les programmes qui peuvent être exécutés en fonction des profils utilisateurs ou administrateurs afin d'éviter que les serveurs de fichiers ou les bases de données ne soient chiffrés. Il est également recommandé de limiter les droits d'écriture sur les serveurs de fichiers afin de réduire la quantité de données pouvant être chiffrées par un ransomware.
- **Renforcer la sécurité informatique en télétravail**: Si les employés de votre entreprise ont droit au télétravail, il est essentiel de bien séparer les outils professionnels et les outils personnels. Si votre entreprise a paramétré un ordinateur avec des accès sécurisés, des

firewalls et autres antivirus, seul cet équipement doit être utilisé. Les employés doivent aussi communiquer exclusivement via des messageries professionnelles sécurisées et entrer dans un espace de télétravail digital protégé par un mot de passe fort et/ou une double authentification. Mettre en place des outils du type réseau VPN pour les flux professionnels permet de sécuriser les échanges et évite qu'un ordinateur personnel devienne une passerelle d'abordage pour les pirates informatiques.

- **Préparer un plan de communication de crise**: En cas d'une attaque de ransomware, votre infrastructure de messagerie et de téléphone peut être perturbée. Il y a donc lieu de préparer des canaux de communication hors ligne. Conservez des copies imprimées des numéros de téléphone portable essentiels (des fournisseurs informatiques, des équipes d'assistance, etc.)
- **Consulter la plateforme de MISP du CIRCL**: CIRCL (Computer Incident Response Center Luxembourg) offre la possibilité à une organisation privée de se connecter à MISP (« Malware Information Sharing Platform »), une plateforme de partage d'informations sur les logiciels malveillants et les menaces existantes. L'objectif de MISP est d'améliorer les contre-mesures utilisées contre les attaques ciblées et de mettre en place des actions préventives et de détection.