La nouvelle loi sur la protection des données est valable pour tous

À partir du 1er septembre 2023, une nouvelle loi sur la protection des données, nettement plus stricte, entre en vigueur en Suisse. Franco Odermatt de BOLL Engineering explique dans une interview ce que cela signifie pour les entreprises et comment les solutions de cybersécurité peuvent les aider.

La nouvelle loi suisse sur la protection des données (en abrégé nLPD) est entrée en vigueur récemment. Quelles en sont les conséquences pour les entreprises suisses?
Bonne question, car beaucoup ne savent pas ce qu'il faut faire concrètement ni même si la nLPD les concerne. Mais tout est clair comme de l'eau de roche: la nouvelle loi sur la protection des données s'applique à toutes les entreprises et à toutes les organisations qui traitent d'une manière ou d'une autre des données à caractère personnel. Toutes doivent analyser leur situation et mettre en œuvre la nLPD dans la mesure du possible.

«Dans la mesure du possible» – qu'est-ce que cela signifie?
Même une petite entreprise artisanale doit protéger les données de ses clients – or, il n'est sans doute pas raisonnable d'y consacrer les mêmes ressources qu'une grande multinationale, par exemple en engageant un responsable dédié à la protection des données. Par ailleurs, la protection des données est souvent moins complexe pour une PME, dont les données sont relativement peu nombreuses et clairement localisées, que pour une grande organisation avec de nombreux collaborateurs et sites.

Quelles données doivent être protégées?
Toutes les données personnelles sont en principe considérées comme sensibles, par exemple les listes de clients avec noms, adresses et autres informations, les rendez-vous avec les clients et les partenaires commerciaux, les dossiers médicaux et les données biométriques. En revanche, les données qui ne concernent que l'entreprise elle-même – des listes de prix et des informations sur les produits en passant par les concepts et les stratégies – ne sont pas protégées par l'État.

Franco Odermatt est product manager et connaît parfaitement les solutions de cybersécurité.

Que signifie la protection des données dans ce contexte?
Il faut veiller à ce qu'aucune donnée sensible ne puisse tomber entre des mains non autorisées – par exemple en cas de vol de données lors d'une attaque de ransomware ou tout simplement en cas de perte d'une clé USB. Si cela se produit, la loi prévoit une obligation de notification: la fuite de données doit être →

communiquée aux personnes concernées et annoncée aux autorités, par exemple au Centre national pour la cybersécurité (NCSC), au Préposé fédéral à la protection des données et à la transparence (PFPDT) ou à la police. La Confédération, qui dispose d'un vaste dispositif de spécialistes, ne peut intervenir qu'à cette condition.

Quelles sont les conditions préalables pour que la protection des données soit efficace?
Tout d'abord, une classification des données doit permettre clairement de savoir où et comment – éventuellement de manière cryptée – quelles données sont stockées, ce qu'il en advient dans les différents processus commerciaux et qui doit avoir accès à quelles données. Comme les activités commerciales sont aujourd'hui souvent largement numérisées, la mise en œuvre de la nLPD influence aussi directement l'informatique. Chaque entreprise doit réfléchir à la manière dont elle doit intégrer la loi en interne. On parle ici de gouvernance des données. Il faut par exemple pouvoir documenter la manière dont se déroule une suppression de données et s'assurer qu'elle a effectivement eu lieu, y compris toutes les sauvegardes.

Comment BOLL Engineering soutient-il l'application la nLPD?
En tant que distributeur, nous proposons à nos partenaires et à leurs clients des solutions de cybersécurité qui, en fin de compte, sont toutes destinées à la protection des données et ne s'arrêtent en aucun cas aux basiques indispensables comme le pare-feu ou la protection des terminaux. Les solutions de SEPPmail ou de Proofpoint, par exemple, permettent de sécuriser le trafic des e-mails. Les solutions PAM (Privileged Access Management), comme celles de Wallix ou de Fudo, garantissent un contrôle d'accès précis et permettent de surveiller et d'enregistrer toutes les activités des utilisateurs internes et externes – ce qui est important pour l'obligation de documentation. Il est tout aussi important de sensibiliser les collaborateurs au phishing et aux autres méthodes d'attaque. Des formations régulières de sensibilisation à la sécurité, proposées par différents fournisseurs, permettent d'atteindre justement cet objectif.

Et quelle aide la Confédération propose-t-elle?
La Confédération a formulé une norme minimale en matière de TIC (technologies de l'information et de la communication) à laquelle il faut absolument se conformer. La norme contient un modèle Excel avec 108 critères qui permet d'évaluer la situation actuelle et d'obtenir des propositions de solutions. Le standard minimum est décisif en cas de plainte civile pour violation de la protection des données: s'il n'est pas respecté, des amendes élevées peuvent être infligées. Et celles-ci – beaucoup l'ignorent – ne sont pas payées par l'entreprise, mais personnellement par les responsables de la protection des données.

BOLL
IT Security Distribution

BOLL Engineering SA
En Budron H15
1052 Le Mont-sur-Lausanne

Tél. 021 533 01 60
vente@boll.ch
www.boll.ch

→ **boll.ch**