UBS et la Cybersécurité

La fréquence d'attaques cybernétiques de complexité croissante contre le secteur financier a considérablement augmenté, et cette tendance va certainement se poursuivre. UBS est en contact avec ses partenaires commerciaux, avec les régulateurs et les contrôleurs de l'application des lois ainsi qu'avec les spécialistes d'intelligence industrielle afin de combattre ces développements et ces menaces d'attaques de plus en plus sophistiquées.

UBS a intensifié ses investissements en matière de cybersécurité au cours de ces dernières années en attribuant d'importantes ressources à l'infrastructure de contrôles de sécurité de l'entreprise et à l'élaboration de programmes combattant ces menaces.

UBS utilise des principes de contrôle approuvés pour traiter de la cybersécurité. Notre approche s'appuie sur cinq piliers essentiels.

Confidentialité des données
Les processus et technologies sont conçus pour protéger les données contre des divulgations non autorisées ou inappropriées. En sus de la protection des données des clients, UBS prend des mesures pour protéger les données sensibles telles que la propriété intellectuelle, les informations financières non publiées et les données personnelles.

Données à caractère privé
Les processus et technologies contribuent aux efforts d'UBS pour satisfaire aux obligations légales, réglementaires et contractuelles de protection des données personnelles, ce qui peut comprendre la protection des données des clients et/ou des collaborateurs.

Sécurité informatique
Les processus et technologies sont conçus pour protéger la confidentialité, l'intégrité et la disponibilité des informations traitées électroniquement.

Gestion des menaces cybernétiques
Les processus et technologies sont conçus spécifiquement pour protéger la banque contre les attaques cybernétiques telles que le déni de services, les fraudes externes et le vol de données.

Sécurité physique
Les processus et technologies sont conçus spécifiquement pour protéger les infrastructures de réseaux et de stockage des données sur les sites où les données d'UBS et des clients sont traitées et entreposées.

UBS associe les mesures ci-dessus avec un cadre formel de gouvernance et de gestion des risques, qui comprend de multiples niveaux d'évaluation des risques internes et externes aussi bien que des processus de recherche et de traitement des risques opérationnels connus. UBS examine les mesures de sécurité de ses fournisseurs externes connectés à son réseau ou ayant accès à des données confidentielles.

UBS s'engage à attirer l'attention de ses collaborateurs et à fournir des informations sur les mesures de protection et de défense efficaces afin d'atténuer les risques relatifs aux menaces cybernétiques.

Afin de réaliser ses objectifs de sécurité, UBS compte sur la contribution de ses clients, à savoir qu'ils jouent leur rôle en adhérant aux exigences contractuelles et aux directives qui s'appliquent aux mesures de sécurité et à l'accès en ligne des produits et services fournis par UBS.

Informations complémentaires
Pour un complément d'information sur les dispositions prises par UBS en matière de sécurité des informations et de gestion des menaces cybernétiques, veuillez-vous adresser à votre Relationship Manager.