UBS und Cybersicherheit

Die Digitalisierung durchdringt unser Leben immer stärker. In dem Masse, in dem Technologien unseren Alltag in Daten umwandelt, sind wir zunehmend auf zuverlässige und sichere Technologie angewiesen, die uns vor modernen Bedrohungen schützen. Diese Anforderung ist vor allem im Bereich Finanzdienstleistungen wichtig. Cyberbedrohungen nehmen zu und werden immer raffinierter. UBS investiert daher kontinuierlich in die Cyber- und Informationssicherheit.

Für die Bekämpfung von Cyberbedrohungen wendet UBS ein breites Spektrum von internen und externen Massnahmen an, die sich an globalen Branchenstandards sowie regulatorischen und gesetzlichen Vorgaben orientieren. Diese Massnahmen decken fünf wichtige Aktivitäten ab:

Analysieren
Verstehen der Bedrohungslage. Die Basis dazu bilden Prozesse, Technologien, der Austausch mit anderen Finanzdienstleistern, Informationsdiensten sowie Strafverfolgungs- und Regulierungsbehörden. Die Analyse hilft, bekannte Bedrohungen als Geschäftsrisiko zu erkennen, Prioritäten zu setzen, auf Unternehmensebene Entscheidungen zu treffen und Investitionen zu tätigen.

Schützen und Vorbeugen
Errichtung mehrstufiger - von aussen nach innen verlaufend - Verteidigungslinien und Kontrollmechanismen für die physische Umgebung, die Perimeter, die interne Infrastruktur und die Daten. Entwicklung, Implementierung und Instandhaltung von Massnahmen, welche die Verfügbarkeit, Integrität, Vertraulichkeit und den Datenschutz der unternehmenseigenen Informationssysteme gewährleisten und die Anforderungen des Unternehmens, der Kunden und der Aufsichtsbehörden erfüllen.

Erkennen
Nutzung von Informationen und moderner Technologien, um Bedrohungen zu erkennen, die auf einen Angriff hinweisen, Sicherheitsvorfälle zu korrelieren und Sicherheitswarnungen auszulösen, damit ein globales Expertenteam mit den Untersuchungen beginnen kann.

Reagieren
Das Unternehmen auf Sicherheitsvorfälle vorbereiten und dafür sorgen, dass Mitarbeiter und die Geschäftsleitung zeitnah reagieren und den Schaden für das Unternehmen, die Kunden und die Stakeholder begrenzen können.

Wiederherstellen
Sobald die Sicherheitsvorfälle geklärt sind, werden die kritischen Dienste und die relevanten IT-Systeme wieder

vollumfänglich hergestellt, um unsere Geschäftsziele zu erreichen.

Diese Aktivitäten sind in einen formellen Risiko- und Governance-Rahmen eingebettet, der von einem internen Governance-Board überwacht wird, welches sich aus Mitgliedern der obersten Führungsebene aller Unternehmensbereiche und Kontrollfunktionen zusammensetzt. Risiken durch interne Prozesse, externe Dritte und andere Abhängigkeiten fliessen in unsere mehrstufigen internen und externen Risikoeinschätzungen ein. Dieses Vorgehen gewährleistet eine umfassende Berücksichtigung aller involvierten Stellen und gewährleistet, dass die Kontrollen der Cyber- und Informationssicherheit kontinuierlich gestärkt werden.

UBS fördert eine Kultur, die zur Cyber- und Informationssicherheit beiträgt. Die Bank sensibilisiert ihre Mitarbeiter kontinuierlich für diese Themen und stattet sie mit dem erforderlichen Wissen aus, damit sie ihre Aufgaben im Hinblick auf Datenschutz und Datensicherheit bestmöglich erfüllen können.

Sie als Kunde können Ihren Teil dazu beitragen, um ein optimales Sicherheitsniveau zu erreichen. Halten Sie sich an die Richtlinien und vertraglichen Verpflichtungen in Bezug auf Sicherheitsmassnahmen – einschliesslich des Online-Zugriffs auf die von UBS angebotenen Dienstleistungen und Produkte – und wenden Sie anerkannte Kontrollprinzipien in Ihrem Umfeld an. Besuchen Sie unsere Cybersicherheit-Seite für weitere Informationen zum Thema.