

USA update nr 2/2021

Dziś kolejny „USA update”, czyli przegląd tego co dzieje się w prawodawstwie w Stanach Zjednoczonych, jak wygląda praktyka regulatorów i jakie nowe inicjatywy podejmowane są przez kluczowych regulatorów dla rynku finansowego i kapitałowego (OCC, FED, SEC, FINRA, CTFC i inni). USA Update nr 2/2021 czyli subiektywnie wybrane przeze mnie newsy „zza Oceanu”:

1. FED/OCC/FDIC – wytyczne dla banków: zarządzanie ryzykiem w relacjach z podmiotami trzecimi

FED/OCC oraz The Federal Deposit Insurance Corporation (FDIC) opublikowały wytyczne w zakresie zarządzania ryzykiem związanym z relacjami z podmiotami trzecimi, w tym relacjami z podmiotami zajmującymi się technologiami finansowymi. Wytyczne to bardzo ciekawy dokument a przy tym mocno kompleksowy. Z ciekawych kwestii wskazano np. dla ryzyka braku zgodności, że banki nie powinny wchodzić w relacje z podmiotami trzecimi, które mają nieodpowiednie procesy zarządzania ryzykiem braku zgodności a jeśli już w taką relację wejdą to powinny monitorować takie firmy, aby zapewnić, że odpowiednio wdrażają obowiązujące przepisy, regulacje i wytyczne dotyczące ochrony konsumentów.

FDIC to niezależna agencja federalna utworzona w 1933 r. w celu wspierania stabilności systemu finansowego poprzez promowanie dobrych praktyk bankowych w szczególności w zakresie bezpieczeństwa depozytów na wypadek upadłości banków oraz kas oszczędnościowych.

Wytyczne dostępne są: [TUTAJ](#).

2. SEC – kolejny oskarżony za insider dealing

Chociaż w przypadku SEC nie jest to nowość, regulator ten znany jest z szybkiego i sprawnego „wymierzania sprawiedliwości” osobom dokonującym manipulacji na rynku oraz tym, którzy stosują praktyki ogólnie pojętego insider dealing’u (wykorzystaniu informacji) to tym razem sprawa jest podwójnie ciekawa. Apostolos Trovias,

obywatel Grecji, został oskarżony o popełnienie przestępstwa wykorzystania informacji oraz udzielania porad na tej bazie "insider trading tips" w przestrzeniach Dark Web (czyli dostępnej z poziomu Darknet „ukrytej części Internetu”). Dark Web ułatwia zachowanie anonimowości (choć pełną anonimowość jak widać niekoniecznie da się osiągnąć). Apostolos Trovias, który w Dark Web występował pod pseudonimem „TheBull, w latach 2016 – 2021 udzielał wskazanych „porad” na forach w Dark Web, ale rzecz jasna nie za darmo. „Byk” wpadł na pomysł sprzedawania wskazanych informacji, tak jednorazowo, jak i poprzez pakiety tygodniowe i miesięczne (sprzedał ponoć ponad 100 subskrypcji). Dobrze przeczytać, że regulatorzy śledzą także zasoby Dark Web (co nie powinno być nowością). Od dawna słyszy się także o służbach wewnętrznych banków, które sprawdzają zasoby Dark Web, by poznać techniki i sposoby jakie wykorzystują przestępcy.

3. DOJ/DHS – StopRansomware.gov

DOJ (The U.S. Department of Justice) i DHS (the U.S. Department of Homeland Security) stworzyły wspólnie z innymi agencjami stronę StopRansomware.gov w celu pogłębiania świadomości w zakresie cyberataków, tak by zwiększyć ochronę amerykańskich firm i obywateli przed cyberatakami. StopRansomware.gov to kompleksowe centrum zasobów oprogramowania anti-ransomware dla osób fizycznych, firm i innych organizacji. Na stronie można znaleźć także całą masę zasobów typu The Ransomware Response Checklist, Ransomware Protection and Response czy Preparing for a Cyber Incident. StopRansomware.gov to pierwszy centralny „węzeł” konsolidujący zasoby oprogramowania ransomware ze wszystkich federalnych agencji rządowych. StopRansomware.gov zawiera zasoby i treści z „Agencji Bezpieczeństwa Cybernetycznego i Infrastruktury” (CISA), DHS i US Secret Service, FBI, Krajowego Instytutu Standardów i Technologii (NIST) i wielu innych.

p.s. nazwy regulatorów amerykańskich I to, czym się zajmują tłumaczyłem w „[USA update nr 1/2021](#)”.