Rozhovor s Monikou Zahálkovou, výkonnou ředitelkou České bankovní asociace

Aktivity České bankovní asociace v oblasti digitalizace

Od listopadu 2020 jste výkonnou ředitelkou České bankovní asociace, která byla založena v roce 1992 a v současnosti má 37 členů, kteří reprezentují 99 % českého bankovního sektoru. Jaké jsou vaše hlavní úkoly a vize v této nové funkci?

Česká bankovní asociace je na trhu již téměř 30 let a stojí za ní velký kus práce. Za tuto dobu se nemalou měrou zasloužila o dobrou pověst českého bankovního sektoru a je také její zásluhou, že veřejnost bankám důvěřuje. A důvěra, jak všichni víme, je v bankovnictví klíčová. Na tuto práci chci jednoznačně navázat a i nadále se aktivně podílet na rozvoji českého bankovního sektoru a celé naší ekonomiky, jakožto i finanční gramotnosti Čechů. Navíc je mým záměrem vytvořit z ČBA svěží, dynamickou a moderní organizaci, která tak bude vnímána napříč celým bankovním trhem, veřejnou správou, ale i širokou a odbornou veřejností.

Banky dlouhodobě patří k lídrům trhu v oblasti inovací a digitalizace. Na požadavky klientů reagují rychle a pružně, jejich obsluhu přizpůsobují jejich stále náročnějším požadavkům. Pokud má být ČBA bankám důvěryhodným a rovnocenným partnerem, musí s nimi držet krok. Musí kopírovat jejich dynamický vývoj, sledovat nejnovější trendy, umět přijímat a využívat moderní technologie a též se aktivně podílet na přinášení inovativních řešení v oblasti bankovnictví. První kroky už jsme v této oblasti udělali. Spustili jsme nový čtrnáctidenní newsletter pro všechny, které bankovnictví zajímá. Také jsme uvedli nový diskusní pořad ČBA FOCUS. Do něj si zveme zajímavé osobnosti z bankovnictví, ale i třeba ze státní správy, a dáváme jim pod vedením zkušeného moderátora prostor pro objektivní diskusi nad aktuálními tématy. První díl už máme za sebou a zasvětili jsme ho digitalizaci českého státu a jak s ní pomáhají banky. Pořad je ke zhlédnutí na našem YouTube kanále nebo si ho můžete poslechnout jako podcast na Spotify. Další novinky chystáme i v oblasti vzdělávání, ale zatím je brzy cokoliv prozrazovat.

Ještě ve vaší předchozí funkci ředitelky Institutu členů správních orgánů CoID jsem absolvoval velmi zajímavý seminář o kybernetické bezpečnosti. Jaká je podle vašeho názoru znalost kybernetických rizik mezi členy top managementu českých firem a jakou prioritu dávají opatřením pro jejich minimalizaci?

Monika Zahálková *vystudovala Vysokou školu ekonomickou v Praze. Působila jako jednatelka CG Institutu a ředitelka Institutu členů správních orgánů (Czech Insstitute of Directors). Mezi lety 2018 až 2019 byla členkou představenstva mediálního domu Economia. Od listopadu 2020 zastává funkci výkonné ředitelky České bankovní asociace.*

V průběhu let se situace zlepšuje. Stále jsou sice organizace, které do kybernetické bezpečnosti investují méně, než by měly, v obecné rovině však tento typ hrozeb vnímají takřka všichni. Zejména korporace se zahraničním vlastníkem mají zkušenost s kybernetickými incidenty a umí si spočítat, že výpadek jejich služeb či provozu je stojí mnohem více, než kolik stojí nástroje na posílení kybernetické bezpečnosti. Vědí, že nejde jenom o náklady na odstranění útoku, ale také o hrozbu ztráty dat, únik osobních údajů, citlivých informací a další s tím související následky.

Zejména telekomunikační operátoři, finanční instituce a obecně společnosti zalistované na některém z kapitálových trhů či společnosti s diverzifikovaným portfoliem služeb a náročným investičním

profilem vědí, že jeden kybernetický útok může na dlouhou dobu zastavit jejich činnost či je z podnikání prakticky vyřadit. Také proto v jejich výročních zprávách vidíte velmi často zmínku o kybernetických hrozbách na jednom z prvních míst potenciálních rizik. Prakticky neznám žádného vysoce postaveného manažera z velké korporace, který by kybernetické hrozby bagatelizoval a nechtěl je řešit.

Prevence obecné finanční a kybernetické kriminality je jednou ze čtyř hlavních oblastí činnosti, které o sobě ČBA uvádí na svých webových stránkách. Co to konkrétně představuje?

Naše zaměření, nejenom v této oblasti, vyplývá z potřeb našich členů, ale také z potřeb veřejnosti. Na jedné straně tedy budujeme společně se státem odpovídající legislativní prostředí, regulační

rámec, který umožňuje bankovnímu sektoru budovat prostředí důvěry, bez kterého nelze úspěšně finanční služby poskytovat. A to jak v oblasti standardní, řekněme fyzické, bezpečnosti, tak i na úrovni mezinárodní spolupráce při potírání kybernetické kriminality. Na straně druhé se společně snažíme působit na klienty, kteří se zejména v dnešní době, kdy se celá řada našich aktivit přesunula do kyberprostoru, stávají cílenými objekty velmi sofistikovaných útoků. Jde o to, abychom je dokázali nasměrovat k uvědomění, že jejich málo obezřetné chování a nízká ochrana jejich elektronických zařízení vede k tomu, že právě oni jsou v drtivé většině právě tím nejslabším článkem v zabezpečení jejich finančních prostředků.

Jak ČBA spolupracuje v této oblasti se státními institucemi, jako je Policie ČR, FAÚ, NÚKIB, ÚOOÚ apod.?

K mé velké radosti velmi úzce. Nerada bych v rozhovoru vyzdvihovala jednu konkrétní instituci. Obecně platí, že spolupráce s regulátory funguje nejenom ve formální, ale i neformální rovině. A to téměř každodenně. Pokud budu přeci jen konkrétnější, tak například s Policií ČR má asociace podepsáno memorandum o vzájemné spolupráci a nastavení komunikace nejenom v oblasti prevence. S institucemi, které jsou pro banky regulátory v oblasti kybernetické bezpečnosti, tedy s Českou národní bankou a s Národním úřadem pro kybernetickou bezpečnost, jsme také pravidelně v kontaktu. Obě tyto instituce s námi v minulých letech spolupracovaly např. při realizaci testů připravenosti bank na řešení masivnějších hackerských útoků zaměřených na bankovní sektor. Zástupci Finančního analytického úřadu, státního zastupitelství a Policie ČR jsou pravidelnými hosty zasedání Komise pro bankovní a finanční bezpečnost, na kterých se zástupci bank diskutují nejen legislativní změny a z nich vyplývající povinnosti v oblasti boje s praním špinavých peněz a financováním terorismu, ale i poznatky z proběhlých útoků – ať už na pobočky, bankomaty či elektronické platební systémy, nebo přímo na klienty. Nesmím také zapomenout zmínit, že ČBA ve spolupráci s FAÚ také pravidelně školí v oblasti praní špinavých peněz a kyberbezpečnosti zaměstnance bank.

Jak je ČBA aktivní v oblasti prevence finanční a kybernetické kriminality například formou vzdělávání, seminářů metodické podpory apod.?

Jak už jsem naznačila, prevence finanční a kybernetické kriminality je nedílnou součástí naší činnosti. Již přes dvacet let pořádáme odborný seminář „Prevence finanční kriminality“, kde si s odborníky v této oblasti vyměňujeme řadu užitečných poznatků. Ty se pak snažíme uplatnit nejenom v práci příslušných útvarů bank, ale také je přenést do vzdělávacích programů a projektů, které ČBA pravidelně připravuje pro širokou veřejnost, od dětí po seniory. Každoročně také měříme tzv. Index kyberbezpečnosti ČBA. Jeho cílem je zjistit, jak si Češi v oblasti kyberbezpečnosti stojí, a na základě těchto výsledků se pak zaměřit na jejich cílenou edukaci. V loňském roce dosáhli Češi ve zmíněném testu jen asi 60% úspěšnosti, v praktickém kvízu dokonce pouze 43 %. Z výsledků vidíme, že nejvíce jsou ohroženi mladí, kteří si nebezpečí nepřipouštějí a také nemají tolik životních zkušeností. Z těchto důvodů ve spolupráci s našimi členskými bankami každoročně organizujeme projekt Bankéři do škol, kdy se zaměstnanci bank vydají tuto problematiku formou interaktivních workshopů vyučovat do středních a základních škol po celé České republice. Projekt má velký úspěch a každý rok se nám do něj zapojuje stále více škol, i když loni nám to pandemie trochu zkomplikovala...

V oblasti finanční bezpečnosti, konkrétně pak fyzické bezpečnosti, také ČBA realizovala v minulosti projekt „Lekce komisaře Maigreta“. Cílem tohoto projektu bylo vytvořit školící videa pro zaměstnance bank, reagující na v té době vysoký nárůst případů loupežných přepadení na území ČR. Toto školení je v bankách využíváno dodnes.

Jak je tato oblast důležitá pro vás osobně, setkala jste se někdy s nějakým bezpečnostním incidentem, se kterým nás můžete obecně seznámit?

Ani já nejsem výjimkou a již jsem se, asi jako každý, s phishingovými útoky setkala. Tyto útoky mají mnoho podob, od podvodných e-mailů sepsaných špatnou češtinou, až po bohužel v poslední době i velmi sofistikované a cílené kriminální aktivity. I já jsem zjistila, že existují podvodné e-shopy plné atraktivního zboží s úžasnými slevami, jejichž jediným cílem je získat od vás údaje o vaší platební kartě za účelem jejího zneužití.

Našim programátorům se podařilo hacknout náš robotický vysavač tak, že nám teď při auditu pomáhá vést auditorský spis.

Kresba: Ivan Svoboda

V poslední době se objevuje nový fenomén tzv. vishing, který je obzvlášť zákeřný, protože pracuje s vašimi emocemi. Jedná se o útoky v podobě telefonických hovorů pachatelů, kteří se vydávají za pracovníky bank. Útočníci volají pod záminkou, že banka zjistila útok na klientův účet nebo platební kartu s tím, že je nutné s jeho pomocí provést jejich okamžité zablokování. Cílem těchto útoků je klienta nejprve dostatečně vyděsit, tedy vyvolat v něm pocit, že jsou aktuálně ohroženy jeho úspory a následně mu sdělit, že vše je možné s jeho okamžitou pomocí ještě zachránit. Klient tak po prvním šoku nabývá pocit spásy, že mu chce jeho banka pomoci a s volajícím začne spolupracovat. Ve snaze ochránit své finance pak prozradí všechny přístupové údaje. Ty přitom banky po svých klientech nikdy nevyžadují. Kromě toho banky samy, pokud například identifikují riziko možnosti zneužití platební karty klienta, tyto karty blokují a žádné údaje od klienta k jejich zablokování znát nepotřebují.

Osobně se zájmem sleduji projekt „Bankovní identita“, ve kterém je ČBA aktivní a který nabízí veřejnosti možnost elektronické identifikace prostřednictvím bankovní identity i do nebankovních informačních systémů, například i do Portálu občana apod. V jaké fázi se projekt aktuálně nachází?

Tento projekt považuji za jeden z nejvýznamnějších za několik posledních let. V loňském roce jsme po dvouletém úsilí dokončili jeho legislativní rámec a do začátku letošního roku jsme ve spolupráci s Ministerstvem vnitra, Ministerstvem financí a Správou základních registrů pracovali na implementaci. To vše vyústilo ve zdokonalení náročného akreditačního procesu, který banky, jakožto poskytovatelé bankovní identity, musí podstoupit v souladu se zákonem o elektronické identifikaci. Akreditaci získalo již pět bank, které nyní ověřují a registrují identitní prostředky svých klientů prostřednictvím státní Národní identitní autority NIA. To probíhá postupně. Denní kapacita systému umožňuje registrovat maximálně 50 tisíc identit. Přesto už jich je od začátku roku více než dva miliony převážně od dvou bank. S trochou zjednodušení tedy můžeme říct, že stejně snadno, jako se přihlašují do internetového bankovnictví, se nyní mohou prokazovat i ve světě ostatních, nebankovních online služeb přes dva miliony klientů.

Bankovní identitu mohou klienti používat při přihlašování na portály státu – samozřejmě jen tam, kde jim to stát umožní. Poslední novinkou je možnost podat daně prostřednictvím portálu Moje daně Ministerstva financí. Dalším připravovaným projektem je Sčítání lidu 2021. Za nejlepší rozcestník, kde si klienti mohou pomocí bankovní identity vyřídit nejrůznější záležitosti směrem ke státu online, považuji Portál občana, kam Ministerstvo vnitra postupně přidává další a další služby a šetří nám tak cesty na úřady.

Pokud tomu dobře rozumím, tak se funkce bankovní identity budou postupně otevírat i pro komerční využití společnostmi, které provozují informační systémy vyžadující spolehlivou elektronickou identifikaci uživatelů (například e-shopy apod.). Jak to bude fungovat?

Podle informací, které máme, se bankám podařilo dosáhnout shody na vybudování jednoho společného podniku Bankovní identita a.s. – BANK ID, jehož prostřednictvím banky firemnímu sektoru nabídnou jedno řešení pro spolehlivou, rychlou a bezpečnou online identifikaci jejich klientů či zákazníků a mimo to také elektronický podpis. Díky tomu tak bude například mobilní operátor či poskytovatel energií po uzavření smluvního vztahu s tímto „agregátorem“ moci vybudovat pouze jedno standardizované technologické rozhraní a jeho prostřednictvím tak spolupracovat se všemi bankami, které budou identitní služby poskytovat. Jsem optimista a věřím, že se bankám a společnosti Bankovní identita vše podaří připravit tak, abychom mohli bankovní identitu v soukromém sektoru používat již počátkem druhé poloviny letošního roku.

Co byste na závěr vzkázala či poradila auditorům s ohledem na bezpečnost využívání ICT osobně i u svých klientů?

V prvé řadě se řídit bezpečnostními doporučeními provozovatelů IT systémů, bank, mobilních operátorů, zkrátka všech institucí, jejichž výrobky a služby využíváme. Těch bezpečnostních opatření není moc, v principu se opakují, ale pokud je dodržujeme, ochráníme tím nejen naše data a soukromí, ale i data našich klientů, kteří nám je s důvěrou svěřili. A tuto důvěru bychom neměli zklamat.

Rozhovor vedl
Ladislav Mejzlík