Kyberbezpečnost aneb společně jde vše lépe

Bankovní byznys je založený především na důvěře klientů, kteří vkládají do banky peníze s tím, že věří, že jsou v bezpečí. Se stejným pocitem dávají bance také své údaje. Proto dnes, v době, kdy je téměř vše digitální a elektronické, je tolik důležité, aby banky dbaly na kyberbezpečnost, která se stává jedním ze stěžejních témat bankovnictví.

Aby byla kybernetická bezpečnost ještě více zajištěna a finanční instituce mohly lépe předcházet kybernetickým útokům, reportují dle směrnice o bezpečnosti sítí a informačních systémů (NIS), která byla přijata v roce 2016 Evropským parlamentem, tyto útoky vybraným bezpečnostním týmům na národní úrovni. V případě České republiky se jedná o bezpečnostní týmy Vládní CERT, provozovaný nově vzniklým úřadem NÚKIB, a Národní bezpečnostní tým CSIRT.CZ, provozovaný sdružením CZ.NIC.

Zatímco Vládní CERT má na starosti především incidenty týkající se kritické infrastruktury, pod kterou spadají např. státní instituce a některé banky, tým CSIRT.CZ spolupracuje na řešení incidentů z ostatních koncových sítí.

Nad národní úrovní existuje spolupráce také na evropské úrovni. Ta funguje primárně ve dvou skupinách, které rovněž vzešly z dané směrnice. Jde o skupinu pro spolupráci a síť CSIRT. Ve skupině pro spolupráci jsou primárně zástupci úřadů jednotlivých členských států, které řeší implementaci NIS směrnice do národních legislativ. Současným cílem skupiny je totiž právě dohlížet na co nejharmonizovanější transpozici směrnice do národních legislativ, která by měla být dokončena v květnu tohoto roku.

Síť CSIRT se pak skládá z členů bezpečnostních týmů, kterým jsou kybernetické bezpečnostní incidenty hlášeny. Tato skupina vznikla spíše z potřeby koordinované reakce na incidenty, které by mohly ohrozit více členských států současně. Prozatím se první rok fungování dané skupiny nesl v operačním duchu, protože si skupina musela definovat pravidla fungování a způsob komunikace. Jako poměrně efektivní se ale ukázalo sdílení informací v případě incidentů, jakým byl například v roce 2017 útok WannaCry. Rychlá reakce jednotlivých členských států umožnila operativně a rychle vytvořit obraz, nakolik byly jednotlivé členské státy zasaženy, což pomohlo k následnému řešení škod. I přesto se i nadále pracuje na vylepšení způsobu sdílení informací mezi bezpečnostními týmy, což je vzhledem k tomu, že týmy v jednotlivých státech mají již zaběhnuté své vlastní systémy, poměrně náročný úkol. Tato oficiální spolupráce mezi členskými státy při výměně informací ohledně incidentů

Nad národní úrovní existuje spolupráce také na evropské úrovni. Ta funguje primárně ve dvou skupinách, které také vzešly z dané směrnice. Jde o skupinu pro spolupráci a síť CSIRT.

však ještě neoslavila ani rok a dá se očekávat, že se bude postupně zlepšovat.

Na evropské úrovni již pak také léta funguje například TF-CSIRT, který zastřešuje bezpečnostní týmy ze státního, akademického či soukromého sektoru. Zde výměna informací funguje již léta. Jde tu však primárně o sdílení know-how a best practice jednotlivých týmů. I zde jsou k dispozici komunikační nástroje, avšak ty jsou využívány méně často, protože plošné incidenty vyžadující úzkou mezinárodní spolupráci se odehrávají jen velice zřídka.

Kybernetická rizika aktuální nejen pro banky

Experti se shodují, že pro banky představuje největší riziko chování uživatelů. Banky pochopitelně investují do zabezpečení svých systémů a neustále zlepšují své procesy spojené s bezpečností. Na druhé straně bezpečnosti bankovních aplikací pak stojí uživatel, který je často tím nejslabším článkem bezpečnosti. Když bychom to chtěli nějak připodobnit, pokud budu zločinec a budu mít na výběr mezi možností vlézt do objektu otevřenými dveřmi, nebo rozbít okno chráněné alarmem a riskovat, že se ještě poraním, nejspíše si vyberu otevřené dveře.

Z tohoto důvodu jsou nejčastějším terčem útoků právě koncoví uživatelé. Právě s těmito útoky má Národní tým CSIRT.CZ největší zkušenosti. Dá se říci, že útočníci využívají různě sofistikované útoky, od phishingových stránek umístěných na zjevně nesmyslné URL přes phishingové stránky na vlastní doméně s platným certifikátem napodobující skutečnou adresu banky až po nejrůznější malware.

Velmi zajímavý byl útok, který se v uplynulých letech objevil v Polsku, v České republice i jinde ve světě. Ten využíval různé chyby,

případně slabá hesla u domácích routerů. Poté co útočník pronikl do routeru, změnil v něm nastavení DNS serveru na server ovládaný útočníkem. Tímto způsobem pak dokázal ovlivnit všechna zařízení, která byla za daným routerem připojena. V sousedním Polsku tak uživatelé, kteří se při připojení přes takovýto napadený router pokusili navštívit stránky například mBank.pl, skončili na stránkách útočníka. Z pohledu uživatele však adresa vypadala správně, neboť skutečně byl na stránce mBank.pl. Jen díky manipulaci útočníka s DNS byla tato stránka mBank.pl provozována na serveru útočníka. Pokud se uživatel na této stránce pokusil přihlásit, získal útočník přístup do jeho internetového bankovnictví. V České republice byl pak tento útok proveden poněkud sofistikovaněji, kdy útočník přesměrovával uživatele využívající napadený router na falešné webové stránky Seznam.cz a Google.cz. Na těchto stránkách pak zobrazil upozornění na nutnost stažení nové verze Flash Playeru, který jim také hned nabídl ke stažení. Problém byl, že místo aktuální verze Flash Playeru byl uvnitř bankovní trojský kůň.

Řešení tohoto plošného útoku je zároveň pěknou ukázkou spolupráce mezi národním CSIRT a bankovním sektorem. V rámci této spolupráce CSIRT předal bankám seznam zranitelných routerů, respektive veřejných IP adres, na kterých se tyto routery nacházely, a banky pak tento seznam využívaly pro odhalování podezřelých transakcí. Tento útok byl také jednou z motivací pro vznik bezpečného routeru Turris a Turris Omnia.

Z aktuálních problémů, které se v rámci bezpečnostní komunity řeší, stojí za zmínku rizika spojená s používáním mobilních telefonů jako druhého faktoru při ověřování přihlašujících se uživatelů nebo při odesílání plateb. Kromě již známých triků, jako je instalace malwaru, který přeposílá příslušné SMS útočníkovi, nebo manipulace uživatele k přeposlání ověřovací SMS útočníkovi pomocí sociálního inženýrství, se v květnu minulého roku objevil v sousedním Německu útok, který zneužíval známé chyby protokolu SS7. Tento protokol se používá v telefonních sítích pro síťovou signalizaci. Jednotlivé protokoly jsou používány například pro spojování a ukončení telefonních hovorů, směrování volání a zpráv na mobilní telefony, přenos SMS mezi ústřednami a SMS centrem a pro řadu dalších úkolů.

Společnost O2 Telefonica Germany potvrdila, že někteří z jejích zákazníků byli okradeni s využitím dvoufázového útoku, který zneužil právě zranitelnosti v SS7. První fáze útoku byla standardní, tedy rozeslání e-mailů s přiloženým malwarem, který útočníkům zajistil přihlašovací údaje, informace o zůstatku a číslo mobilu. V další fázi pak zaplatili za přístup do sítě jiného operátora a přesměrovali telefon do své sítě. Následně jim již nic nebránilo přihlásit se do bankovnictví oběti dříve získanými přihlašovacími údaji, poslat peníze a odchytit ověřovací SMS, která jim umožnila dokončit převod peněz na jiný účet.

Zachrání uživatele biometrika?

S masivním rozšířením chytrých mobilních telefonů začali klienti bank mnohem častěji využívat pro obsluhu svých bankovních účtů právě mobilní zařízení. Trend je jasný a každoročně počet uživatelů mobilního bankovnictví narůstá.

Banky se tomu musely přizpůsobit, především co se týká zabezpečení autentizace. Z historie je zjevné, že prosté heslo již dávno nestačí a další metody jako např. certifikáty či čtečky jsou zase uživatelsky nepřívětivé, protože uživatel musí stále u sebe nosit něco navíc. Tento problém částečně řeší využívání biometrik, které je stále rozšířenější i díky jeho stále častější hardwarové podpoře v zařízeních. Právě toho banky čím dál častěji využívají.

Pod pojmem biometrický údaj si nejspíš většina z nás ihned představí otisk prstu. Tento údaj je nejčastěji využívaným ze souboru tzv. fyzických biometrik, ale čím dál častěji se objevují experimenty v zabezpečení pomocí kombinace fyzických a tzv. behaviorálních biometrik, které vyhodnocují unikátní vzorce uživatelova chování či interakce se zařízením. Příkladem může být britská banka HSBC, která v minulém roce zavedla možnost autentizace pomocí technologie rozpoznávání hlasu. Taková autentizace neporovnává pouhý zvukový záznam, tedy jakousi fyzickou, resp. hlasovou predispozici, ale mimoto pracuje také se souborem desítek dalších znaků, jako je přízvuk, zvuky, které sami o sobě děláme jazykem či ústy, nebo způsob, jakým dýcháme. Vyhodnocováním těchto specifických znaků je prakticky vyloučena možnost napodobení, protože i kdyby vlastní hlas zněl stejně, šance shody u dalších znaků se limitně blíží nule.

Experimenty s dalšími typy biometrik nás v blízké budoucnosti nejspíš ještě čekají a právě banky budou pravděpodobně jejich průkopníky. Nabízí se možnost autentizace pomocí unikátního tlukotu srdce, specifického proudění krve v žilním systému a dalších jedinečných znaků. Samozřejmě nelze opomenout také v nedávné době uvedenou technologii Face ID společnosti Apple, která rozpoznává obličej uživatele a je postavena na rychle se učící neuronové síti, jež vyhodnocuje další podružné znaky. Tato síť se navíc dokáže učit z vlastních chyb, takže je pravděpodobné, že v budoucnu se bude jednat o velice spolehlivou technologii.

Jenže jak je to s bezpečností? Zachrání biometrický podpis nezodpovědné uživatele? Obecně se dá říct, že biometrika sama o sobě bezpečná je – vždyť se jedná o unikátní a nepřenositelné znaky uživatele. Jak už to ale bývá, i zde je hlavní slabinou uživatel a zabezpečení samotného zařízení.

Pokud se totiž uživatel stane obětí phishingu, malwaru a dalších technik, ani biometrika situaci nezachrání, a měla by tedy tvořit pouze jeden z faktorů přihlášení. Druhým faktorem zde pak může být např. kontrolní SMS kód. Právě kombinace více faktorů riziko celkové kompromitace výrazně snižuje. Jak je tedy vidět, útoky na uživatele internetového bankovnictví mohou mít mnoho různých podob. A pokud se chová uživatel nezodpovědně, ani ten nejbezpečnější systém ho nezachrání. Proto i nadále platí, že dodržování základních bezpečnostních pravidel je klíčové.

B | Text Radka Vařechová, bezpečnostní analytička, CZ.NIC
www.bankovnictvionline.cz

Z aktuálních problémů, které se v rámci bezpečnostní komunity řeší, stojí za zmínku rizika spojená s používáním mobilních telefonů jako druhého faktoru při ověřování přihlašujících se uživatelů nebo při odesílání plateb.