Народна банка Србије нашла се на удару интернет преваранта након што је добила фактуру да плати 175.500 евра са лажне имејл адресе у којој је само једно слово промењено у односу на имејл адресу правог добављача.

С обзиром да је НБС избегла да одговори на конкретно питање Данаса да ли су трансферисали новац, може се претпоставити да су службеници централне банке насели на превару.

Али, колико год нам се чинило да је 175.500 евра пуно, НБС је имала среће, јер тај износ није ништа у поређењу са пљачком централне банке Бангладеша у фебруару 2016. године, када је са њених рачуна код филијале ФЕД-а у Њујорку пребачено 101 милиона долара, од чега је Бангладеш успео да стопира исплату 20 милиона, па им је отето "само" 81 милион долара. Иначе преваранти су тада дали налоге за исплату чак милијарду долара.

У овом случају преваранти су се дочепали сигурносних креденцијала за приступ СWИФТ-у неког од службеника Централне банке Бангладеша уз помоћ којих су 4. фебруара 2016. послали више од 30 налога њујоршком ФЕД-у за исплате милиона долара на рачуне у банкама на Шри Ланци, Филипинима и по другим азијским земљама.

Превара је откривена када су сутрадан службеници централне банке Бангладеша видели да штампач који штампа све трансфере и ради 24 сата дневно није одштампао ништа. Софтвер на том терминалу који је повезан са СWИФТ-ом је показивао да или недостаје или је измењен системски фајл. Када су сутрадан успели да покрену штампач "искочиле" су десетине сумњивих трансакција. У међувремену су из ФЕД-а наводно послали упите за потврду тих трансакција али им у Бангладешу нико није одговарао, па су пустили осам, док су остале блокирали. Када су схватили превару, из Бангладеша су покушали да контактирају Њујорк, али тамо је била субота и до понедељка нису могли да зауставе трансакције. У међувремену до 9. фебруара очишћени су рачуни у банкама по Азији. Неколико дана касније СWИФТ је послао поруке клијентима са упозорењем на преваре, као и да је у неколико случајева дошло до компромитовања приступа СWИФТ систему, мада ови случајеви никада нису стигли до јавности.

Сличне преваре су прошле године покушане и са централном банком Соломонових острва која је послала упозорење да мејлове послате са адресе гувернера ове централне банке не треба отварати, мада нема извештаја да ли је било и преварених.

Према подацима ФБИ-а у последње три године штета од интернет превара предузећа износила је 5,3 милијарде долара. Преварена предузећа су у просеку губила 218.000 долара у овим преварама.

Према речима стручњака за сајбер безбедност оваквих случајева ће бити много више у будућности и јако је битно да се код запослених у компанијама, али уопште и код јавности подигне свест о интернет преварама и интернет безбедности.

Такође, банке, па и централне банке спадају у циљеве високе вредности који доносе велику добит или вредне информације. Највеће светске компаније трпе више милијарди напада или како то зову стручњаци сигурносно интересантних догађаја на месечном нивоу.

Занимљиво је да се најчешће краду или хакују имејл адресе генералних директора компанија, а мете превара су најчешће финансијски директори.

Пали на просту "фору"

Превара са лажном фактуром (богус инвоице сцхеме) чија је жртва НБС је позната одавно и небројено компанија је пало на ову у принципу веома једноставну превару. Превара се обавља тако што се или хакује мејл неког од запослених у предузећу или се

само измени једно слово или број у имејлу са ког се шаљу купцу измењене инструкције за уплату на рачун преваранта.

Други случај превара нема толико везе за технологијом колико са социјалним инжењерингом. Преваранти користе имејл адресу директора (превара се зове ЦЕО превара) и са њега шаљу мејл запосленом углавном у финансијама са налогом да се одређена сума хитно исплати на одређени рачун (преваранта). Преваранти су свесни да запослени када виде директоров мејл не пада им на памет да га проверавају већ се одмах бацају на извршење. С друге стране, директори често немају знања из ИТ-а и посебно безбедности због чега су лаке мете.

Трећи пример је када преваранти хакују налог неког од запослених из компаније и са њега шаљу фактуре са налогом за ургентно плаћање разним купцима које нађу у контакт листи. У четвртом случају, преваранти се представљају као адвокати друге компаније или адвокатске фирме који наводно имају осетљиве материјале и притискају директоре или менаџере фирми да хитно и у тајности изврше уплате. Ова превара се често обавља на крају радног дана или недеље када се запослени спремају да крену кући и онда упадају у панику због неочекиваних проблема.

"У циљу истраге"

Наш лист је јуче замолио НБС за податке о томе да ли су њени службеници исплатили 175.500 евра по лажној фактури, да ли су поднете кривичне пријаве и која се институција бави истрагом овог случаја, да ли је покренута унутрашња истрага у НБС и да ли постоји могућност да се исплаћена средства поврате, али НБС није одговорила ни на једно од тих питања, ради, како су навели, "неометаног вођења истраге".
НБС је навела да се догодио "покушај извршења кривичних дела" и да су о томе обавестили "надлежне органе".

Злоупотребе на старински начин

Централне банке нису имуне ни на оне уобичајене проневере без употребе компјутера. Тако је рецимо у Нигерији 2015. године неколико службеника имало задатак да уништи 40 милиона долара вредан локални новац наира. Они су исецкали гомиле новинског

папира на величину новчаница и њих уништили, а новац задржали и касније пустили у оптицај преко пословних банака па је и 16 службеника ових банака такође ухваћено.

У Кенији је исте године откривена злоупотреба тешка 439 милиона долара која је трајала годинама. Руководиоци приватних банака плаћали су одређеним службеницима централне банке школарине за деци и подмићивали их на друге начине, док су ови заузврат окретали главу на другу страну приликом незаконитих зајмова које су ове банке пласирале, док су у извештајима приказивали да је све у реду.

(Фонет)