Banki bűncselekménytrendek, az ATM és bankkártyatámadások eseményei

Miután az ATM, EGY MAGÁRA HAGYOTT PÉNZTÁROLÓ VÉGPONT bűnözői szempontból, ezért mindig is foglalkoztak vele, hogy mi módon lehetne hozzáférni a pénzhez. Nyilván az eszköz nagyfokú folyamatosan frissülő biztonsága lehűti ezeket a vágyakat, de mindig akadnak újabb kísérletek.

■ ***Az ATM szolgáltatásai, biztonsága***

Az ATM (automatikus kifizető eszköz) egy olyan intelligens banki kifizető végpont, amely alkalmas a bank ügyfelei elektronikus azonosítására, bankkártya és PIN-kód segítségével. Használatával ügyfelünk készpénzhez juthat a nap bármely szakában, és egyéb tranzakciós műveleteket, módosításokat is végrehajthat számlakörnyezetében. (pl. mobil telefonkártya-feltöltés, kódváltás, állítható limitértékek). Az ATM-ek nem választhatóak le a banki hálóról, áram, vagy hálózat hiány esetén nem működnek!

Mechanikailag páncélszekrény szintig megerősített szerkezeti kialakításúak, a behatolásjelző-hálózatba bekötött, videotechnikával felszerelt, telepítési előírások szerint beépített és lerögzített eszközök. Lokális biztonsági rendszerekkel is védettek, ezért helyi riasztást is generálnak megtámadásuk esetén.

■ ***Az ATM-ek típusai***

Az ügyféligények figyelembevétele alapján többféle alaki és elhelyezési kivitelben léteznek. ▸ Fali (külső és belső telepítésű), ▸ Oszlop, vagy sziget típusú eszközök.

■ ***A fizikai támadások történeti fejlődése***

Miután az ***ATM, egy magárahagyott pénztároló végpont*** bűnözői szempontból, ezért mindig is foglalkoztak vele, hogy mi módon lehetne hozzáférni a pénzhez.

Nyilván az eszköz nagyfokú folyamatosan frissülő biztonsága lehűti ezeket a vágyakat, de mindig akadnak újabb kísérletek. A 90-es évek slágere a „ragasztásos" pénzszerzési módszer volt, amely sokáig keserítette életünket. A pénzkiadó nyílások teljes átalakításával e bűncselekmények megszűntek. A következő hullám a kártyaadatok technikai eszközökkel történő megszerzése, másolása és kinyerése volt. Ezzel párhuzamosan európai szinten megkezdődtek az ATM „kirántásos" bűncselekmények, melyek Spanyolországtól Lengyelországig mindenhol, nemzetközi bandák közreműködésével zajlottak. Hazánkban 2009-re teljes mértékben megszűnt e bűncselekményforma, mivel betelepítettük a robbanópatronos védelmet az ATM-ekbe. Szerették ezt az elkövetéstípust a bűnözők, mivel jogilag az ATM-ek kirántása rablás helyett csak különösen nagy értékű ***rongálás, lopás*** bűncselekmény-nek minősül (3–5 év büntetés) szemben a rablás új büntetési tételével (20 évig is mehet).

Műveletileg könnyebben megoldható, mint a bankrablás, hiszen nincs humán kockázata. Próbálkoztak még az ATM-ek felrobbantásával is többször, de ezek sem voltak túl sikeresek, és a robbanópatronos módszer már ez ellen is véd.

■ ***A bankkártya-bűncselekmények***

A bankkártya és a PIN kód az ügyfelet teljes mértékben reprezentálja a pénzkiadó eszközökkel szemben, ezért ezek megszerzése az elérendő cél támadásukkor. Általános védekezési javaslatunk a PIN és a kártya külön tárolásával, valamint a kártyalimitek rugalmas kezelésével a lehetséges veszteségek minimalizálhatóak. A bankkártyákon alkalmazott chip bevezetésével az adatlopás veszélye is jelentősen lecsökkent.

■ ***Kártyabűncselekmény-típusok***

■ *Zseblopással, egyéb, általában tárcalopással együtt* ▸ Ha nincs melléírva a PIN kód az esetben gyors letiltással a veszteség teljes mértékben korlátozható.

■ *Kártyaadat ellopása* ▸ álcázott kártyaolvasóval (fizetőhelyeken, ATM-bejáratnál, ATM-olvasónyíláson, komplett leolvasó rendszerrel ATM-helységben.) ▸ Komplex adatcsomaglopás.

■ *Nagy adattároló helyek feltörésével,* összesen két esetben fordult elő ezidáig, de nyilván a kárviselő ilyenkor nem az ügyfél, hanem a kellő gondosságot mellőző adatgazda. (Pl: Adatbázis illegális megszerzésével Amerikai kiberbűnözők két nagybank hitelkártya-adatbázisát feltörve 45 M dollár kárt okoztak. RAKBANK, MUSCATBANK)

■ *ATM-környezeti támadások:* erőszakos vagy trükkös pénzelvételek fordulhatnak elő az eszköz környezetében. Ezért javasolt pénzfelvételkor kellő körültekintéssel ezt végrehajtani.

■ *NET-es kártyafosztogatások*

A NET-vásárlás ürügyén, a felhasznált bankkártyák lefosztásával. Érdemes e célra külön számlát és kártyát létrehozni, amit csak erre használunk. Vásárlási szándék esetén csak azt az összeget tesszük elérhetővé a számlán, amit erre szánunk, így védekezhetünk az illegális lehívás ellen.

■ *ATM-ből adatlopás speciális belső adatgyűjtő eszközzel*

Ez is nemzetközi hullámban Irországból induló bűncselekmény volt, az ATM eszközoldalát kivágva, egyéb speciális eszközöket telepítve az ATM-helységbe, komplex adatcsomagokat és PIN-eket szereztek meg, majd Dél-Amerikába juttatva ezeket onnan fosztogattak velük. Itt Budapesten buktak le, köszönhetően a szoros együttműködésnek.

■ *„Reverse" bűncselekmények*

Valós kártyával román bűnözők ez évben már többször próbálkoztak e bűncselekménytípussal. Egy speciális eszköz használatával működésében korlátozzák, megrongálják az ATM-et egyszeri pénzhez jutás reményében. Már több ilyen bűnözőt megfogtunk a szoros együttműködés eredményeképen.

■ ***A megelőzés lehetséges útjai***

▸ A felbukkanás, felderítés adatainak gyors megosztása, illetékes együttműködő körökben ▸ Az elkövetés lehetőségét biztosító körülmény, hiba gyors felszámolása ▸ Hatósági együttműködés gyakorlati formáinak kialakítása, a felszámolás érdekében. ▸ ATM-gyártó-, üzemeltető cégekkel szoros együttműködés, a hibaokok gyors technikai felszámolása érdekében.

Fialka György