KÉSZÜLT: 2023 SZEPTEMBER

KIBERTÁMADÁSOK KORA

KIBERBIZTONSÁG ÉS A FIZETÉSEKET ÉRINTŐ CSALÁSOK A PÉNZÜGYI ÖKOSZISZTÉMÁBAN

BEVEZETÉS

A pandémia utáni időszak egyik legfelkapottabb témája a digitalizáció evolúciós ugrása és ennek hatásai a mindennapi életünkre. A digitalizáció okozta számos újítás mellett van negatív vonatkozása is ennek, amelyre nagyobb figyelmet kellene szentelnünk: a kiberbűnözés és a fizetési csalások számottevő növekedése.

Mivel a világjárvány során mindennapi életünk és rutinjaink nagy része az internetre került, a kiberbűnözők egyre fejlettebb és hatékonyabb eszközöket használnak arra, hogy megtalálják a digitális ökoszisztémában lévő sebezhetőségeket. 2020-ban több biztonsági jogsértés történt, mint az elmúlt 15 évben összesen, és ez a szám 2021-ben további 17%-kal emelkedett.

A csalók és a hackerek elleni küzdelemhez a régióban egységes erőfeszítésre van szükség, mivel a különálló szervezeteknek csak korlátozott rálátása van a fenyegetésekre. Az együttműködés és a partnerségek lehetővé teszik, hogy közösen találjuk meg a kiberbűnözés elleni küzdelem leghatékonyabb módjait.

A Mastercardnál nap mint nap azon dolgozunk, hogy a kibervédelem élvonalában legyünk és ezzel segítsük az iparág valamennyi érdekeltjét, és hatékony megoldásokat nyújtsunk a kibertámadások és a fizetési csalások megelőzéséhez.

Bár napról napra egyre több kockázati tényezőt látunk felbukkanni, én mégis optimistább vagyok, mint valaha, hogy együtt forradalmasíthatjuk az adatvédelem területét.

Ennek a tanulmánynak az a célja, hogy áttekintést adjon a jelenlegi fenyegetésekről, meghatározza a kiberbiztonság és a csalás elleni védelem legfontosabb kihívásait, bemutassa, hogyan lehet kezelni és megelőzni ezeket a támadásokat, és ismertesse, hogy a Mastercard változatos megoldásai hogyan vehetik le a terhet az Ön válláról, hogy Ön a digitális fejlesztésekre és innovációkra tudjon összpontosítani.

Remélem, hogy ez a tanulmány hozzájárul a kiberbiztonságról szóló vitákhoz az Ön szervezetében. Ha bármilyen kérdése vagy visszajelzése van, azt örömmel fogadjuk.

Üdvözlettel,
PAOLO BATTISTON
Executive Vice President, Services, Europe

ANTROPOLÓGIAI ÁTTEKINTÉS

A HOMO DIGITALIS BEMUTATÁSA

A Homo Digitalis, vagyis a digitális kor embere kényelmesen eligazodik a mindennapokban a modern technológiával. Bár használják az online eszközöket, nem értik teljesen, hogyan működnek. Nem veszik észre a leselkedő veszélyeket, és pánikba esnek, ha baj van. Sokan tévesen azt hiszik, hogy a megoldás a digitális világtól való elszakadásban rejlik, pedig hangsúlyozni kell a digitalizáció és a technológiai fejlődés elkerülhetetlenségét.

Globális, jól felszerelt hackerhadseregek indítanak támadásokat a digitális birodalom ellen. Általában a Homo Digitalis sokkal sebezhetőbb ezekkel a támadásokkal szemben, mivel nem érti a technológiai fenyegetéseket. A Homo Digitalis az offline létben keres menedéket, nem tudván, hogy a digitális fejlődést nem lehet elkerülni. A vállalkozásoknak többnyire láthatatlan, de jól felkészült partnerekre van szükségük, akik képesek megvédeni őket a hackertámadásoktól.

Ezek a védelmi szakértők képesek azonosítani a támadásokat és hatékonyan reagálni a kiberbűnözők által támasztott kihívásokra. Ők a digitális világ rejtett őrei, akik védelmet nyújtanak a Homo Digitalis csoportok számára a kibertámadások növekvő támadásai ellen.

A KIBERBŰNÖZŐK STRATÉGIÁT VÁLTANAK. ÖN LÉPÉST TART VELÜK?

A digitalizáció visszafordíthatatlan folyamat, amely egyre inkább fejlődik, és következésképpen **NÖVELI A HOMO DIGITALIS SEBEZHETŐSÉGÉT.** Ebben a világban **HACKERNEK LENNI OLCSÓ.** A megfizethető, csúcstechnológiás megoldások mindenki számára elérhetőek. Ugyanakkor a digitális világ összetettsége folyamatosan növekszik, ami **EGYRE TÖBB POTENCIÁLIS FENYEGETÉST** eredményez, ami új védelmi intézkedéseket igényel. A hackerek **MINDIG ÚJ GYENGE PONTOKAT KERESNEK:** a legújabb trendek szerint **EZEK MA MÁR A RENDSZEREKET HASZNÁLÓ EMBEREK ÉS A BESZÁLLÍTÓK.**

A megelőzés kulcsszereplői a **VÁLLALATOK** - ha körültekintőek és kellően felkészültek, rendszereik biztonságban lesznek a globális támadásokkal szemben, beleértve a nagyszabású támadásokat is.

E TANULMÁNY CÉLJA, HOGY BEMUTASSA, HOGYAN HASZNÁLJÁK KI A KIBERBŰNÖZŐK EZEKET A GYENGESÉGEKET, ÉS JAVASLATOKAT TESZ AZ ELLENÜK VALÓ VÉDEKEZÉSRE.

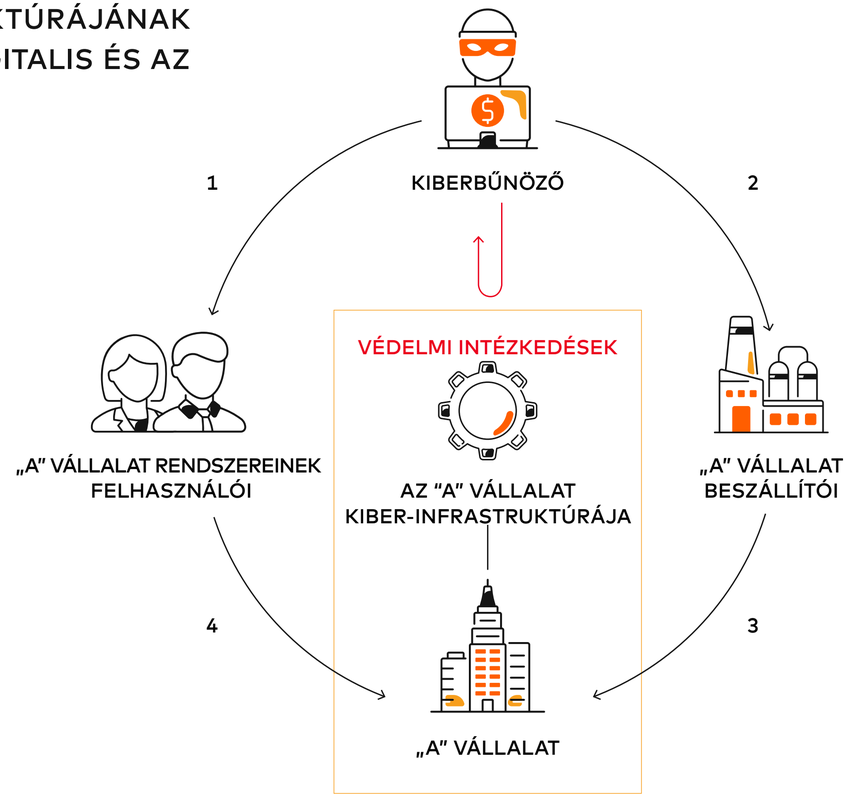
A tanulmány számos forrás felhasználásával készült, többek között az EKB és az MNB tanulmányai, az iparági szakértőkkel készített interjúk, valamint **A MASTERCARD SAJÁT KIBERBIZTONSÁGI MEGOLDÁSAI SZOLGÁLTAK ALAPUL,** globális lefedettséget biztosítva.

AZ ÚJ STRATÉGIA AZ ÚJ

GYENGE PONTOK

KIHASZNÁLÁSÁRÓL SZÓL

A KIBERBŰNÖZŐK MINDIG A GYENGE PONTOKAT KERESIK. MIKÖZBEN EGYRE TÖBB VÉDELMI INTÉZKEDÉS BIZTOSÍTJA A VÁLLALATOK INFRASTRUKTÚRÁJÁNAK BIZTONSÁGÁT, A HACKEREK A HOMO DIGITALIS ÉS AZ ELLÁTÁSI LÁNCOK ELLEN FORDULNAK.



1 Manapság, ha egy kiberbűnöző meg akarja támadni az „A" vállalatot, valószínűleg nehéz feladat elé néz: **A VÁLLALATOK ERŐSEN VÉDIK KIBERINFRASTRUKTÚRÁJUKAT.**

2 A kiberbűnözők azonban még mindig 2 irányban támadhatnak: **AZ „A" VÁLLALAT RENDSZEREINEK FELHASZNÁLÓI** és az **„A" VÁLLALAT BESZÁLLÍTÓI** felé.

3 Ha az „A" vállalat **BESZÁLLÍTÓI NEM RENDELKEZNEK MEGFELELŐ KIBERBIZTONSÁGI INTÉZKEDÉSEKKEL,** és a **NEM FOGNAK MEGFELELNI** az olyan szabályozásoknak, mint a **DORA** vagy a **NIS2,** az „A" vállalat veszélyben van.

4 Ha az infrastruktúra védett, a kiberbűnözők **MÁS GYENGE PONTOKAT KERESNEK,** amelyek közül az egyik **AZ EMBERI TÉNYEZŐ, A HOMO DIGITALIS.** Ezt a **SOCIAL ENGINEERING** segítségével tudják kihasználni.

AGENDA

1. FEJEZET

KIBERBŰNÖZÉS ÉS BIZTONSÁG

KIBERBŰNÖZÉS EURÓPÁBAN ÉS MAGYARORSZÁGON

KIBERBIZTONSÁG LEGFONTOSABB KIHÍVÁSAI

2. FEJEZET

FIZETÉSEKET ÉRINTŐ CSALÁSOK

FIZETÉSEKET ÉRINTŐ CSALÁSOK EURÓPÁBAN ÉS MAGYARORSZÁGON

FIZETÉSEKET ÉRINTŐ CSALÁSOK LEGFONTOSABB KIHÍVÁSAI

KIBERBŰNÖZÉS & BIZTONSÁG

1. FEJEZET

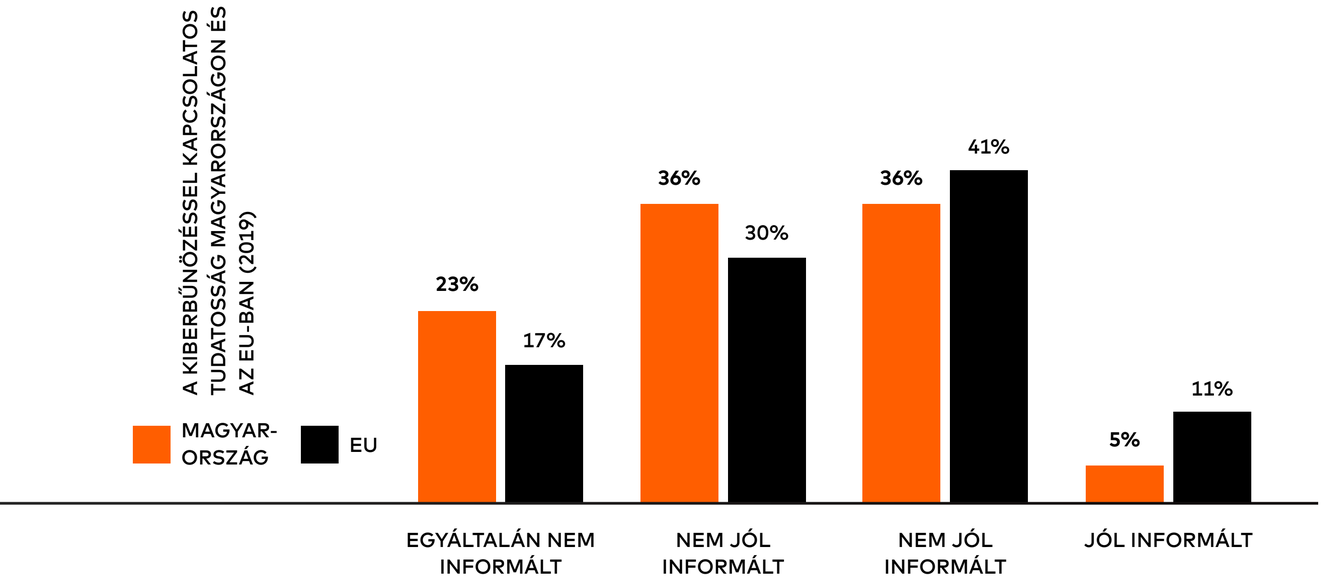
A KIBERBŰNÖZÉS ÁTTEKINTÉSE

EURÓPÁBAN ÉS MAGYARORSZÁGON

MAGYARORSZÁG EGYRE NAGYOBB FENYEGETÉSSEL NÉZ SZEMBE

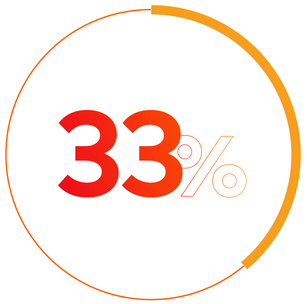
A MAGYAR LAKOSSÁG KÖRÉBEN

ALACSONY A KIBEBŰNÖZÉSSEL KAPCSOLATOS TUDATOSSÁG

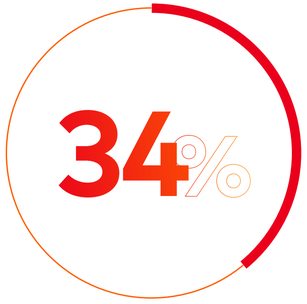


Az adatvédelmi incidensek, kibertámadások száma egyre nő, ugyanakkor **A MAGYAROK TÖBB MINT FELE NINCS MEGFELELŐEN INFORMÁLVA A KIBERBŰNÖZÉS KOCKÁZATAIRÓL,** ami jelentősen elmarad az uniós átlagtól. Magyarországon majdnem minden negyedik embernek nincs információja vagy ismerete a kiberbűnözésről, és csak 5%-uk állítja, hogy nagyon jól tájékozott ilyen kérdésekben. Az Európai Unióban a tudatosság jelentősen magasabb, ami azt jelzi, hogy **MAGYARORSZÁGNAK JELENTŐS JAVÍTANIVALÓJA VAN A FELHASZNÁLÓK KIBERBIZTONSÁGGAL KAPCSOLATOS FELVILÁGOSÍTÁSÁBAN.**

A kiberbűnözéssel kapcsolatos alacsony tudatosság mellett **A MAGYAROK TÖBBSÉGE** azt állítja, hogy **NEM JELENTENÉ A KIBERBŰNÖZÉST:** csak minden harmadik magyar jelentené, ha személyes adatait ellopták volna, vagy ha online banki csalás áldozatává vált volna. A kiberbűnözéssel kapcsolatos általános ismeretek hiánya, valamint az adatlopás és csalás bejelentésére való alacsony hajlandóság a helyi ügyfeleket kiszolgáltatottabbá teszi a kiberbűnözőkkel szemben. Ez a jelenség a Homo Digitalis gondolkodásmódját tükrözi: bár használja a szükséges eszközöket, megelőlegezi a harmadik fél általi védelmet.



A MAGYAROK NEM JELENTENÉK BE A SZEMÉLYES ADATOK ELLOPÁSÁT*

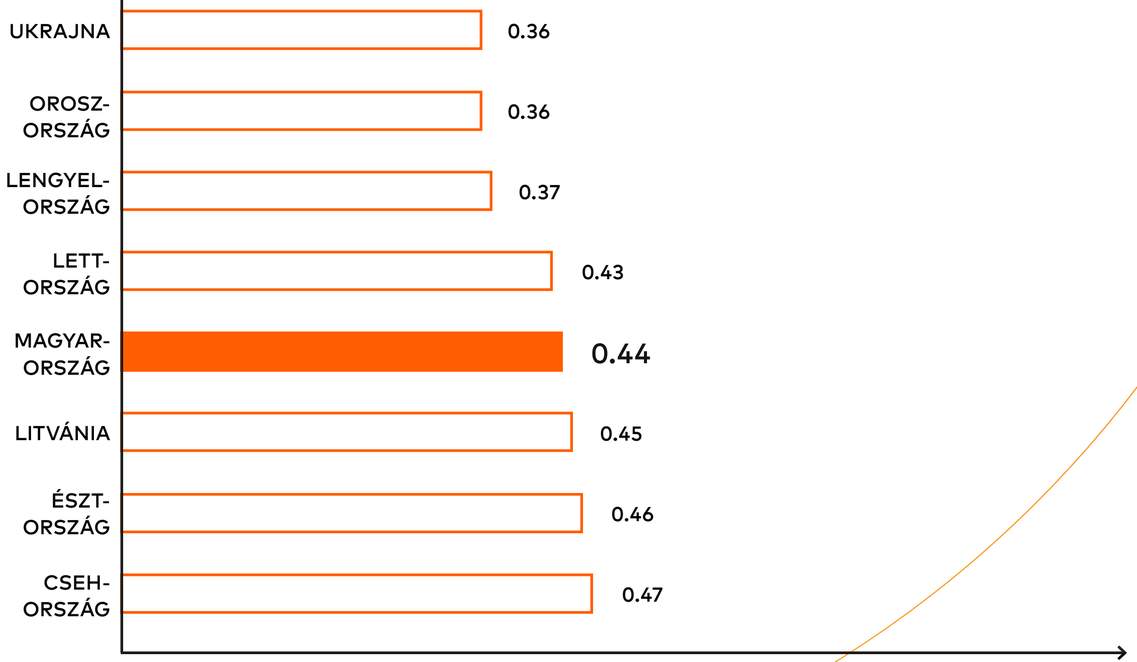


A MAGYAROK NEM JELENTENÉNEK ONLINE BANKI CSALÁST*

Források: Profilics Testing

A KIBERKOCKÁZAT

A KÜSZÖBÖN ÁLL: A KIBERKOCKÁZAT, A BÉREK ÉS AZ ONLINE TÖLTÖTT IDŐ KÖZÖTTI ÖSSZEFÜGGÉS



KIBERKOCKÁZAT INDEX CEE ORSZÁGOKBAN (2020)

MAGYARORSZÁG A KÖZÉP- ÉS KELET-EURÓPAI RÉGIÓ ORSZÁGAI KÖZÜL A NEGYEDIK LEGMAGASABB KITETTSÉGI RÁTÁVAL RENDELKEZIK, ÉS MÉRSÉKELT KIBERKOCKÁZATNAK VAN KITÉVE.

A fejlettebb technológiai infrastruktúrával rendelkező, magas jövedelmű országokban nagyobb a kiberbűnözés kockázata. A legfontosabb tényezők:

AZ ONLINE ELTÖLTÖTT IDŐ MENNYISÉGE
alapján, a több időt online töltők nagyobb veszélyeknek vannak kitéve.

A MAGYAROK ÁTLAGBAN NAPI 1-2 ÓRÁT TÖLTENEK ONLINE.

A MAGASABB BÉREK
lehetővé teszik a bűnöző számára hogy magasabb értékű csalásokat kövessenek el.

Jegyzetek: A kiberkockázati index (CRI) a lakóhely szerinti ország alapján jelzi előre a kiberbűnözés áldozatává válás kockázatát, ahol a 0 pontszám azt jelenti, hogy nincs kiberkockázat, az 1 pontszám pedig a maximális kiberkockázatot jelenti.
A CRI 14 olyan mutatóból áll, amelyek hozzájárulnak az országszintű számítógépes bűnözéshez, és amelyek társadalmi-gazdasági, digitális, számítógépes és bűnözéssel kapcsolatos tényezőkre vannak kategorizálva.
Források: NordVPN and Statista 2020 CRI Survey

AZ ÜGYFELEK SZEMÉLYES ÉS PÉNZÜGYI ADATAI A LEGVONZÓBB CÉLPONTOK A KIBERBŰNÖZŐK SZÁMÁRA.

MELY IPARÁGAK A LEGVESZÉLYEZTETETTEBBEK?

A személyes és pénzügyi információk begyűjtése érdekében a **KIBER-TÁMADÁSOK CÉLPONTJAI FŐKÉNT AZ ÁLLAMI ÉS PÉNZÜGYI SZEKTOR,** valamint a **KOMMUNIKÁCIÓS ÉS MÉDIAIPAR** voltak Magyarországon.

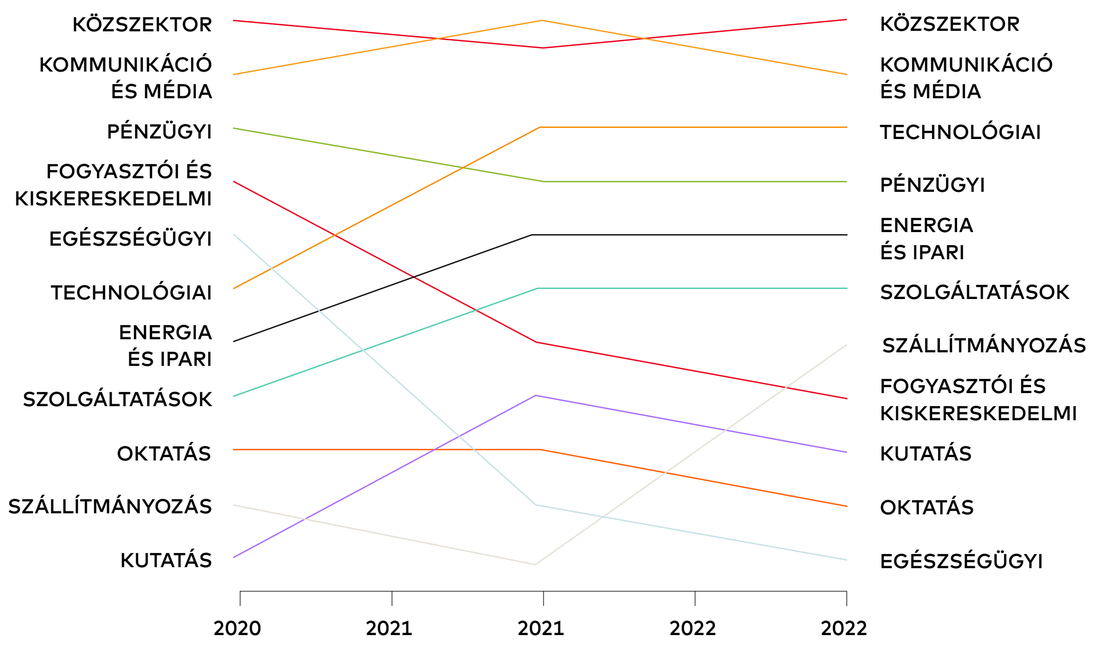
2021-ben a **TECHNOLÓGIAI, AZ ENERGETIKAI ÉS IPARI,** valamint a **SZOLGÁLTATÁSI SZEKTOROK JELENTŐSÉGE NŐTT,** amit 2022-ben a közlekedési ágazat egészített ki, míg a fogyasztói és kiskereskedelmi, valamint az egészségügyi ágazat visszaesett a rangsorban.

KIBERTÁMADÁSOK MAGYARORSZÁGON

FŐ TÁMADÁSI MÓDSZER **47%** a magyarországi támadások nagy része malware-en keresztül történt

LEGGYAKORIBB CÉLPONT **26%** a magyarországi kibertámadásoknak az ügyfelek személyes és pénzügyi adatainak megszerzése a célja

A TÁMADÁSOK MÖGÖTTI LEGGYAKRABB MOTIVÁCIÓ **48%** a magyarországi támadóknak anyagi indíttatású.



Források: Mastercard Cyber Quant platform: 14 adatforrásból gyűjtött adatok, többek között: a Mastercard fenyegetésekkel kapcsolatos információi, kiberbiztonsági eseményekről szóló jelentések, dark webes weboldalak, hackerfórumok, RSS-csatornák.

AZ UKRÁN HÁBORÚ HATÁSA MAGYARORSZÁG KIBERHADVISELÉSÉRE

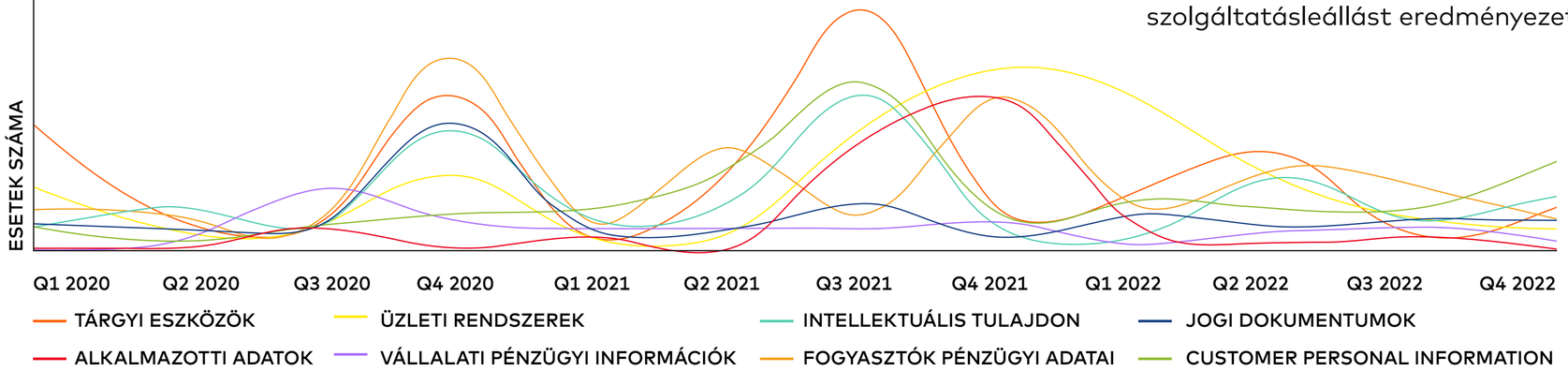
MELY ESZKÖZÖKET FENYEGETI LEGINKÁBB KIBERTÁMADÁS?

A személyes adatokat védő európai szabályozás ellenére 2021 Q3-ban jelentősen **MEGNŐTT A SZEMÉLYES ADATOK ELLENI TÁMADÁSOK SZÁMA.** Egy alacsonyabb aktivitású időszakot követően **2022 Q4-BEN EZEK ISMÉT MEGUGROTTAK,** ami valószínűleg **A NÖVEKVŐ SZÁMÚ CSALÁSOKNAK** köszönhető, mint például a telefonhívások és a hamis weboldalak, amelyek többek között pénzügyi intézményeknek és futárcégeknek adják ki magukat..

A FIZIKAI ESZKÖZÖKET ÉS ÜZLETI RENDSZEREKET CÉLZÓ TÁMADÁSOK mintázata arra utalhat, hogy a támadók célja a kritikus üzleti és működési rendszerek folyamatos megzavarása.

Adataink szerint Magyarországon 2022-ben csökkent a kibertámadások aránya, amit valószínűleg befolyásolhatott az ukrajnai konfliktus, amely átirányította a kiberbűnözői tevékenységeket.

MAGYARORSZÁGI PÉLDA:
A nagyvállalatokat érintő egyik legnagyobb kibertámadásra 2020-ban került sor, amikor az elsősorban pénzintézeteket célzó nemzetközi DDoS[1]-támadás a Magyar Telekom szervereit is elérte. A támadássorozat mértéke és összetettsége ideiglenes szolgáltatásleállást eredményezett.



A LEGGYAKORIBB MAGYARORSZÁGI KIBERTÁMADÁSOK TÍPUSAI

Források: Mastercard Cyber Quant platform, Reuters.com
Mastercard Cyber Quant platform: 14 adatforrásból gyűjtött adatok, többek között: a Mastercard fenyegetésekkel kapcsolatos információi, kiberbiztonsági eseményekről szóló jelentések, dark webes weboldalak, hackerfórumok, RSS-csatornák. 1: A DDOS (Distributed denial of service) támadások célja, hogy egy számítógépes rendszert offline állapotba kényszerítsenek azáltal, hogy egyszerre több számítógépről származó adatokkal árasztják el.

CÉLKERESZTBEN

A HOMO DIGITALIS: AZ E-MAILES SOCIAL ENGINEERING EGYRE NAGYOBB TERET NYER

MILYEN TÍPUSÚ KIBERTÁMADÁSOK FENYEGETIK LEGGYAKRABBAN A HOMO DIGITALIS KÖZÖSSÉGET?

MALWARE

A kártevő szoftverek *(malwarek)* nemkívánatos műveleteket, például adatlopást vagy a számítógép feltörését, végeznek. Leggyakoribb formái a trójaiak, vírusok, férgek és kémszoftverek.

EMAIL SOCIAL ENGINEERING

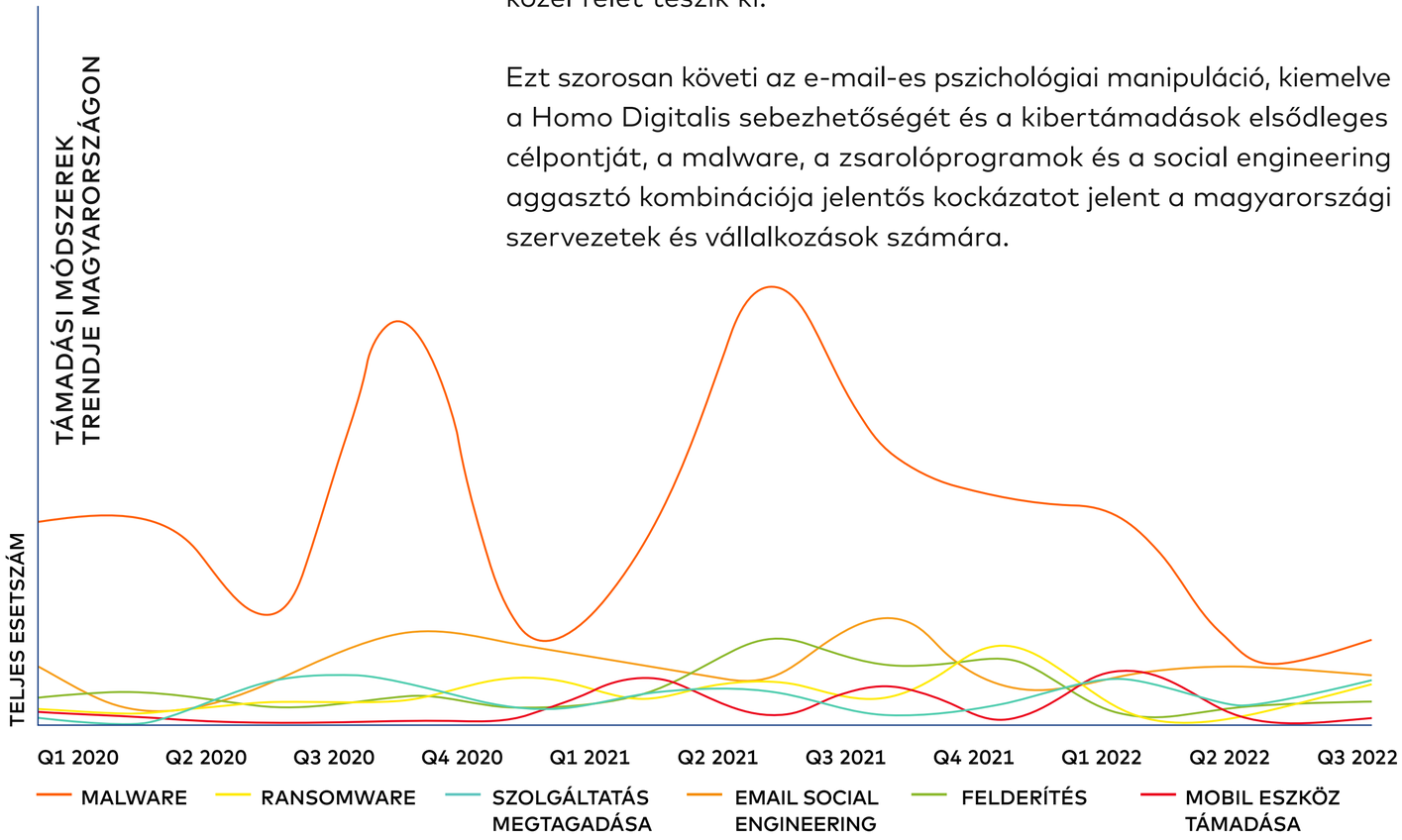
E-mailes pszichológiai manipuláció esetén az elkövető érzékeny adatokat vagy pénzt csal ki az áldozából – ezt teheti spam, hamis e-mailek, adathalászat és/vagy szigonyozás formájában is.

RANSOMWARE

A zsarolóvírus a kártevő szoftverek egy fajtája, amely megfertőzi a felhasználók számítógépét és oly módon manipulálja a rendszert, hogy az áldozat ne férjen hozzá az adataihoz.

Magyarországon a rosszindulatú szoftverek váltak a domináns támadástípussá, amelyek 2020 és 2022 között az összes támadás közel felét teszik ki.

Ezt szorosan követi az e-mail-es pszichológiai manipuláció, kiemelve a Homo Digitalis sebezhetőségét és a kibertámadások elsődleges célpontját, a malware, a zsarolóprogramok és a social engineering aggasztó kombinációja jelentős kockázatot jelent a magyarországi szervezetek és vállalkozások számára.



Források: Mastercard Cyber Quant platforms; Ipsos, Mastercard Cyber Quant platform: 14 adatforrásból gyűjtött adatok, többek között: a Mastercard fenyegetésekkel kapcsolatos információi, kiberbiztonsági eseményekről szóló jelentések, dark webes weboldalak, hackerfórumok, RSS-csatornák.

A KIBERBIZTONSÁG

FŐ KIHÍVÁSAINAK KEZELÉSE

KORMÁNYOK, SZERVEZETEK ÉS VÁLLALATOK ÁLLNAK A KIBER-TÁMADÁSOK FRONTVONALÁN

KIBERTÁMADÁSOK MEGELŐZÉSE: ALAPVETŐ ÉRINTKEZÉSI PONTOK

A BIZTONSÁGI RENDSZEREK NAPRAKÉSZEN TARTÁSA

A BESZÁLLÍTÓK VÉDELMÉNEK BIZTOSÍTÁSA

FOLYAMATOS ÉBERSÉG - ZERO TRUST POLITIKA

A KIBERBIZTONSÁGI KOCKÁZATI KITETTSÉG JOBB MEGÉRTÉSE

Forrás(ok): Mastercard Advisors Analysis

KIBER-BIZTONSÁGI KIHÍVÁSOK:

A BIZTONSÁGI RENDSZEREK NAPRAKÉSZEN TARTÁSA

Ahogy az informatikai rendszerek egyre összetettebbé válnak, a csalók is egyre kifinomultabbá és sokoldalúbbá válnak a módszereikben.

HOGY TÖRTÉNNEK A TÁMADÁSOK?

- A kibertámadások vagy adatvédelmi incidensek előfordulhatnak technikai módszerek vagy emberi hibák révén, akár rosszindulatúak, akár nem rosszindulatúak.

MIT TEHETÜNK ELLENE?

- A biztonsági rendszerek naprakészen tartása.
- **LEGYEN EGY VILÁGOS KÉPÜNK AZ INFORMATIKAI RENDSZEREK BIZTONSÁGÁRÓL ÉS AZONOSÍTSUK A SEBEZHETŐ PONTOKAT.**
- Oktassuk a munkavállalókat a kiberbiztonsággal kapcsolatban.

MILYEN LÉPÉSEKET TEHETÜNK A MEGELŐZÉS FELÉ?

- Az elektronikusan tárolt adatok védelméhez elengedhetetlenek az adatkezelési szolgáltatások, valamint a célzottabb szabályozási erőfeszítések.
- A DORA* például kockázatkezelési küszöbértékeket határoz meg a szervezetek számára a kibertámadások elleni védekezés és azok mérséklése érdekében.

A SZABÁLYOZÁSI ERŐFESZÍTÉSEK A BIZTONSÁGI ELŐÍRÁSOK KOMOLYSÁGÁNAK FEJLŐDÉSÉT IS ELŐSEGÍTHETIK az informatikai biztonsági minimum-követelmények előírásával. **AZ EU JAVASOLT DIGITÁLIS PÉNZÜGYI CSOMAGJA, A DIGITAL OPERATIONAL RESILIENCE ACT (DORA)** a pénzügyi szektor működési rugalmassági keretét jelenti. Egységes követelményeket határoz meg a pénzügyi szektorban működő vállalatok és szervezetek, valamint a számukra IKT-vonatkozású szolgáltatásokat nyújtó kritikus harmadik felek hálózati és információs rendszereinek biztonságára vonatkozóan.

Forrás(ok): EUR-Lex - 32022R2554 - EN - EUR-Lex (europa.eu)

KIBER-BIZTONSÁGI KIHÍVÁSOK:

A BESZÁLLÍTÓK VÉDELMÉNEK BIZTOSÍTÁSA

HOGY TÖRTÉNNEK A TÁMADÁSOK?

- Az adatok kiszervezésével a szervezetek **ELVESZÍTIK A SAJÁT BIZTONSÁGOS INFORMATIKAI RENDSZEREIK ÁLTAL NYÚJTOTT MEGBÍZHATÓ VÉDELMET.** A hackerek azonosítják a kiberbiztonsági lánc **LEGGYENGÉBB PONTJAIT,** ezért létfontosságú a teljes ökoszisztéma biztonságának figyelembevétele.

MIT TEHETÜNK ELLENE?

- **A SZERVEZETEKNEK OLYAN MEGOLDÁSOKAT KELL BEVEZETNIÜK,** amelyek az Egyesült Királyság Nemzeti Kiberbiztonsági Központjához hasonlóan a szabályozó szervekkel együttműködve **KÉPESEK NYOMON KÖVETNI ELLÁTÁSI LÁNCUK CSALÁSNAK VALÓ KITETTSÉGÉT.**

MILYEN LÉPÉSEKET TEHETÜNK A MEGELŐZÉS FELÉ?

- Folyamatos ellenőrzés - **AZ ÉRTÉKLÁNC MINDEN VÁLLALATÁT VÉDENI KELL** a kiberbűnözés ellen.

54%

az adatlopást elszenvedő szervezeteknek 54%-a *(az elmúlt 12 hónapban)* az **ELLÁTÁSI LÁNCUKHOZ TARTOZÓ VÁLLALATNÁL TÖRTÉNT ADATVÉDELMI INCIDENS MIATT SZENVEDETT TÁMADÁST**

"Egy csúcsminőségű biztonsági rendszerrel és riasztóval felszerelt ház semmit sem ér, ha a szomszédnak van egy pótkulcsa, és elveszíti azt. Ugyanez a helyzet az IT-biztonsággal is - a bűnözők a legkisebb ellenállás felé tartanak, ezért gondoskodni kell arról, hogy az ellátási lánc is védett legyen."

MARSI TAMÁS
Lead of Event Detection Team
Nemzeti Kibervédelmi Intézet

Forrás(ok): Mastercard Advisors Analysis; digital-operational-resilience-act.com; Ponemon Institute

KIBERBIZTONSÁGI KIHÍVÁSOK:

FOLYAMATOS ÉBERSÉG: ZERO TRUST POLITIKA

HOGY TÖRTÉNNEK A TÁMADÁSOK?

- **A FELHASZNÁLÓKNAK KÉPESNEK KELL LENNIÜK BÁRHONNAN DOLGOZNI** és biztonságosan hozzáférni a szervezet rendszereihez, miközben az eszközöket és az adatokat jól kell védeni a kiberbűnözéssel szemben. A lényeg: a szervezeteknek meg kell szüntetniük a feltétlen bizalmat a hálózatban.

MIT TEHETÜNK ELLENE?

- A szervezeteknek fel kell mérniük, hogy **A FELHASZNÁLÓK HOGYAN LÉPNEK KAPCSOLATBA DIGITÁLIS ESZKÖZEIKKEL.**
- A zéró bizalom biztonsági házirendek használata a legkisebb jogosultságú hozzáférési modellen alapul. A felhasználóknak "éppen elegendő hozzáférést" biztosítanak a munkájuk elvégzéséhez, és folyamatosan hitelesítik őket a személyazonosságuk és szerepük alapján, függetlenül a tartózkodási helyüktől.

MILYEN LÉPÉSEKET TEHETÜNK A MEGELŐZÉS FELÉ?

- Mindig hitelesítse a felhasználókat, és ellenőrizze az adatokhoz és szolgáltatásokhoz való hozzá-férésüket a legkisebb jogosultság elve szerint.
- A vállalati szolgáltatások és eszközök állapotának felügyelete
- A hozzáférés szabályozása az adott szolgáltatás vagy adat értéke szerint.
- Soha ne bízzon a hálózatokban, még a helyi hálózatokban sem.

MINDEN FELHASZNÁLÓ HITELESÍTÉSE

ÉRVÉNYESÍTSE AZ ÖSSZES ESZKÖZT

ADATHOZZÁFÉRÉS KORLÁTOZÁSA

Forrás(ok): Mastercard Advisors Analysis

KIBER-BIZTONSÁGI KIHÍVÁSOK:

A KIBERBIZTONSÁGI KOCKÁZATI KITETTSÉG JOBB MEGÉRTÉSE

HOGY TÖRTÉNNEK A TÁMADÁSOK?

- Gyakran van szakadék a cégek által a kiberbűnözéssel kapcsolatban észlelt és a tényleges kockázat között. Így előfordulhat, hogy az IT-biztonságról más ügyekre helyezik át a hangsúlyt, ennek következtében a rendszer kiszolgáltatottá válik a hackereknek. A tudatosság hiánya megakadályozhatja a vezetőket abban, hogy megfelelő és elegendő beruházást eszközöljenek a kiberbiztonságba.

MIT TEHETÜNK ELLENE?

- A kibertámadások megelőzése érdekében a szervezeteknek tisztában kell lenniük a birtokukban lévő adatokkal. Ez lehetővé teszi számukra, hogy felmérjék a potenciális kiberbiztonsági kockázatokat és azonosítsák a rendszereik gyenge pontjait. Ezáltal hatékonyabban tudják rangsorolni az IT-biztonságba történő befektetéseiket.

MILYEN LÉPÉSEKET TEHETÜNK A MEGELŐZÉS FELÉ?

- A szervezeteknek alaposan fel kell mérniük kiberkockázati kitettségüket, azonosítaniuk kell a támadásból eredő esetleges pénzbeli és nem pénzbeli veszteségeket, és stratégiai befektetéseket kell eszközölniük a kiberbiztonság javítása érdekében ott, ahol az a legnagyobb hatással jár.

"Bár az elmúlt években történt előrelépés, nagy kihívást jelent elmagyarázni a kiberkockázatot a kkv-knak és a nagyobb szervezeteknek. Biztosítanunk kell, hogy az IT-biztonság a szervezeti kultúra részévé váljon. Ennek egyik módja, ha segítünk a vezetőknek megérteni a vállalatuk kockázati kitettségét, hogy komolyabban vegyék ezt a kérdést."

MARSI TAMÁS

Lead of Event Detection Team

Nemzeti Kibervédelmi Intézet

Forrás(ok): Mastercard Advisors Analysis

HOGYAN SEGÍTHET A MASTERCARD A KIBERBŰNÖZÉS ELLENI

KÜZDELEMBEN?

E KIHÍVÁSOK LEKÜZDÉSÉRE, VALAMINT A VÁLLALATOK ÉS A HOMO DIGITALIS TÁRSADALMÁNAK VÉDELMÉRE A MASTERCARD KÉT FŐ TERMÉKKATEGÓRIÁBAN KÍNÁL MEGOLDÁSOKAT:

MILYEN MEGOLDÁSOK LÉTEZNEK?

A BIZTONSÁGI RENDSZEREK NAPRAKÉSZEN TARTÁSA

A BESZÁLLÍTÓK VÉDELMÉNEK BIZTOSÍTÁSA

FOLYAMATOS ÉBERSÉG - ZÉRÓ BIZALOM POLITIKA

A KIBERBIZTONSÁGI KOCKÁZATI KITETTSÉG JOBB MEGÉRTÉSE

FELHASZNÁLÓ-KÖZPONTÚ

A **NUDETECT** valós idejű védelmet nyújt az online és mobil bankszámlák számára anélkül, hogy megzavarná a felhasználói élményt. Ez a megoldás a digitális banki munkamenet során végig védi a felhasználó teljes útját azáltal, hogy több száz eszköz-, helymeghatározási, passzív biometrikus és viselkedési jelet értékel a korábbi felhasználói viselkedéstípusok alapján. A NuDetect a felhasználók még súrlódás-mentesebb, valós idejű, passzív biometrikus és viselkedési adatokon alapuló validálás-ának lehetővé tételével segítheti a cégeket a zéró bizalomra vonatkozó irányelvek bevezetésében.

IT RENDSZER-KÖZPONTÚ

A Mastercard többféle megelőző megoldással támogatja a bankokat és a kereskedőket a kiberkockázat becslésében és a javítandó területek azonosításában az informatikai biztonsági rendszereik értékelésével.

A **RISKRECON** egy olyan kiberkockázat-értékelő termék, amelynek célja, hogy felmérje, azonosítsa és enyhítse a kiberalapú sebezhetőségeket az ügyfél vállalkozásának digitális ökoszisztémájában, valamint a harmadik felek beszállítói és szállítói rendszerében. A nyilvánosan elérhető információk alapján egyértelmű elemzést nyújt az ügyfél IT-biztonsági felkészültségi szintjéről, összehasonlítja azt az ágazattal és a globális versenytársakkal, és felsorolja azokat a kiemelt fókuszterületeket, amelyeket a szerve-zetnek a fejlesztések érdekében figyelembe kell vennie.

A **CYBER QUANT** egy diagnosztikai felmérés alapján értékeli a jelenlegi kiberbiztonsági kockázatokat, és a kockázatértékelésbe beépíti az aktuális fenyegetettségi helyzetet. Azáltal, hogy számszerűsített értéket ad a jelenlegi kockázatokról és a potenciális veszteségekről, ez az eszköz támogatja a szervezeteket az informatikai és biztonsági területekre irányuló beruházások rangsorolásában.

A **CYBER FRONT** elemzi a szervezet jelenlegi informatikai rendszereit szimulált kiberfenyegetésekre adott válaszaik alapján. Ez az eszköz segít a szervezetnek abban, hogy a gyenge pontok azonosításával, a biztonság folyamatos érvényesítésével, a válaszlépések meghatározásával és a védelem javítá-sával jobban felkészüljön a csalók elleni küzdelemre.

Forrás(ok): Mastercard Advisors Analysis

FIZETÉSEKET ÉRINTŐ CSALÁSOK

2. FEJEZET

A FIZETÉSEKET ÉRINTŐ CSALÁSOK
NEMZETKÖZI ÉS LOKÁLIS

TRENDJEI

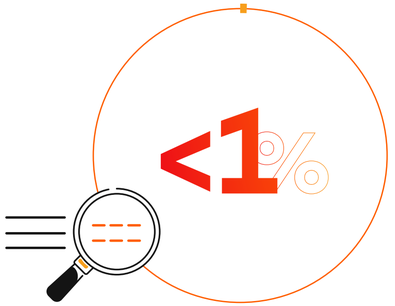
MAGYARORSZÁG EGYRE NAGYOBB
FENYEGETÉSSEL NÉZ SZEMBE

FIZETÉSEKET ÉRINTŐ CSALÁSOK ÁTTEKINTÉSE

AZ ÉVES GLOBÁLIS FIZETÉSI CSALÁS NAGYSÁGA MAGYARORSZÁG ÉVES GDP-JÉNEK EGYÖTÖDÉVEL EGYENÉRTÉKŰ. A fizetési csalások trendjeinek, valamint a megelőzési módszereknek a mélyreható megértésével a szervezetek és a magánszereplők felvértezhetik magukat a szükséges tudással és eszközökkel ahhoz, hogy ellenállóak maradjanak egy olyan világban, amelyet egyre inkább fenyeget a fizetési csalás.

2020-ban **A FIZETÉSI CSALÁSOKBÓL EREDŐ ÉVES GLOBÁLIS VESZTESÉG** meghaladta a **32 MILLIÁRD DOLLÁRT,** ami több mint **TÍZSZERES NÖVEKEDÉST** jelent az elmúlt tíz év során.

Becslések szerint **2027-RE** a globális fizetési csalásokból származó veszteségek elérik a **40 MILLIÁRD DOLLÁRT.** Ez **25%-OS NÖVEKEDÉST JELENT** a fizetési csalásból eredő veszteségek jelenlegi értékéhez képest.



A fizetési csalás elterjedtsége ellenére a fizetési csalással gyanúsított pénzeszközöknek kevesebb mint **1%-ÁT FAGYASZTJÁK BE VAGY FOGLALJÁK LE.** Ez jelentős lehetőségeket jelent a pénzügyi világ szereplői számára: javítani tudják a csaláskezelési módszereiket, jobb üzleti eredményeket érhetnek el és biztonságosabb pénzügyi környezetet teremthetnek.

Forrás(ok): MerchantSavvy; ENSZ Kábítószer- és Bűnügyi Hivatala

KÁRTYATRANZAKCIÓKKAL KAPCSOLATOS CSALÁSOK: A HATÉKONY KIBER-HADVISELÉS JÓ PÉLDÁJA

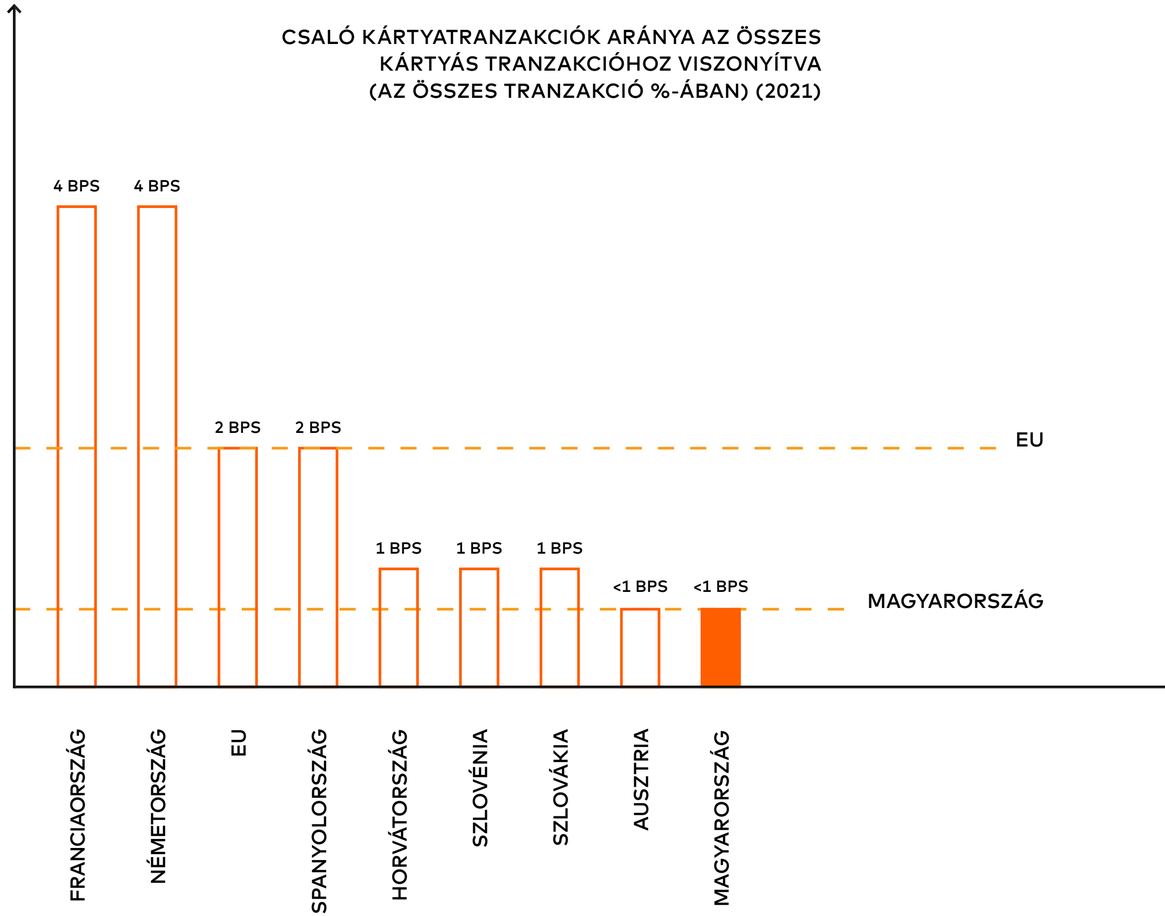
A csalásokból eredő óriási veszteségek ellenére a **CSALÁRD KÁRTYATRANZAKCIÓK ARÁNYA EURÓPA-SZERTE VISZONYLAG ALACSONY**. 2021-ben az **EURÓPAI UNIÓBAN** a csalás aránya a tranzakciók esetében nagyjából 2 bázispont volt.

A KÁRTYACSALÁST HÁROM FŐ TÉNYEZŐ BEFOLYÁSOLJA:

BEVÉTEL: A magasabb átlagjövedelemmel rendelkező országok a kedvező kockázat-haszon arány miatt nagyobb gazdasági ösztönzést nyújtanak a csalók számára.

NYELV: Minél egyedibb a nyelv, annál nehezebb hiteles kártyacsalást végrehajtani.

ALAPVETŐ PÉNZÜGYI ISMERETEK: A képzettebb országokban valószínűleg nagyobb a csalási tudatosság, és kifinomultabb csalásmegelőzési politikák vannak érvényben.

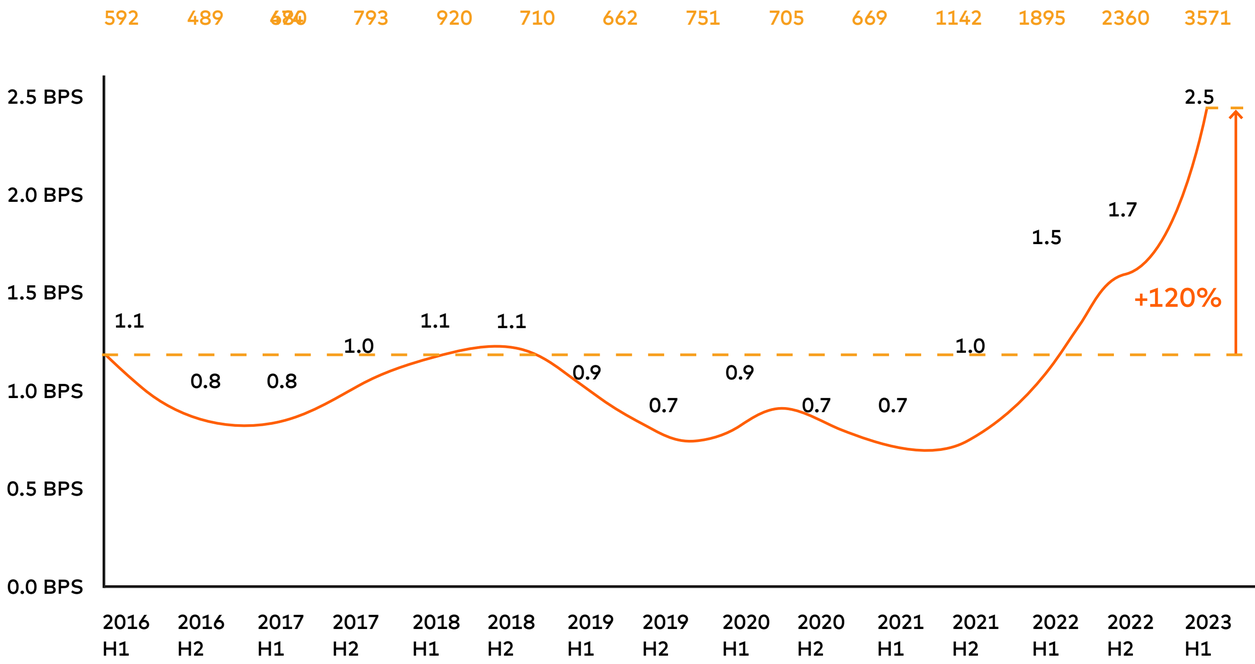


Source(s): European Banking Authority | (europa.eu)

KIS MÉRTÉKBEN NŐ

A KÁRTYÁS FIZETÉSI CSALÁSOK SZÁMA MAGYARORSZÁGON

KÁRTYÁS FIZETÉSI CSALÁSOK ÉRTÉKE MILLIÓ FORINTBAN



Azzal együtt, hogy a kártyacsalások értéke 2017 második féléve óta folyamatosan 500 millió forint felett volt, 2021-ben és 2022-ben meredeken tovább emelkedett. A 2023-as év első felében az érték már meghaladta a 3,5 milliárd forintot. Ezzel együtt a csalási arány is megugrott, 2023 második felében elérte a 2,5 bázispontot.

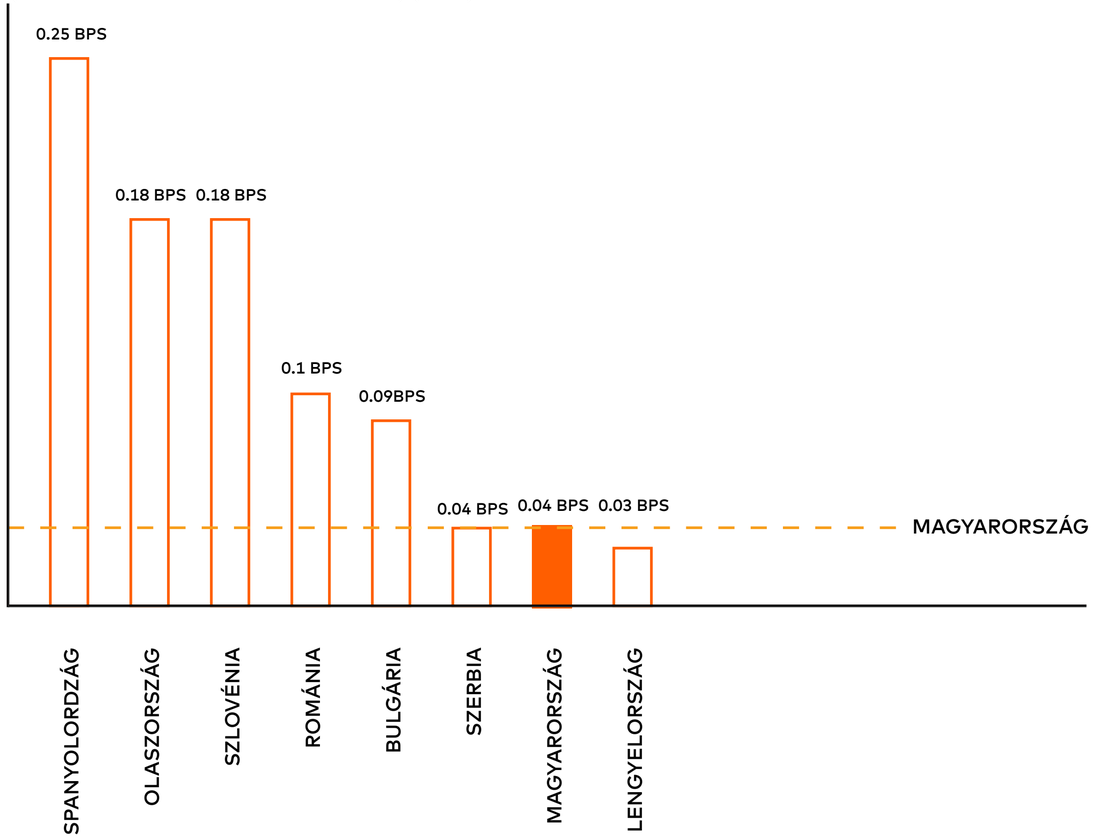
A kártyacsalások számának az elmúlt két évben tapasztalt erőteljes növekedése nagyrészt az új típusú csalások meg jelenésének köszönhető, amelyek a fizetési kártyák hitelesítő adatainak ellopásán túl a Homo Digitalis közösséget is célba veszik a **SOCIAL ENGINEERING** segítségével.

KÁRTYÁS FIZETÉSI CSALÁSOK ARÁNYA ÉS ÉRTÉKE MAGYARORSZÁGON, A KIBOCSÁTÓ SZEMSZÖGÉBŐL NÉZVE (2016 H1 – 2023 H1)
(BÁZISPONT, MILLIÓ FORINT)

Forrás(ok): Magyar Nemzeti Bank (II.6; II.6.d; III.2a; III.2b)

ÁTUTALÁSI CSALÁS

A CSALÁSOK ARÁNYA AZ ÁTUTALÁSOK ESETÉBEN A KIVÁLASZTOTT ORSZÁGOKBAN
(A KIFIZETÉS TELJES ÉRTÉKÉNEK %-A) (2020)



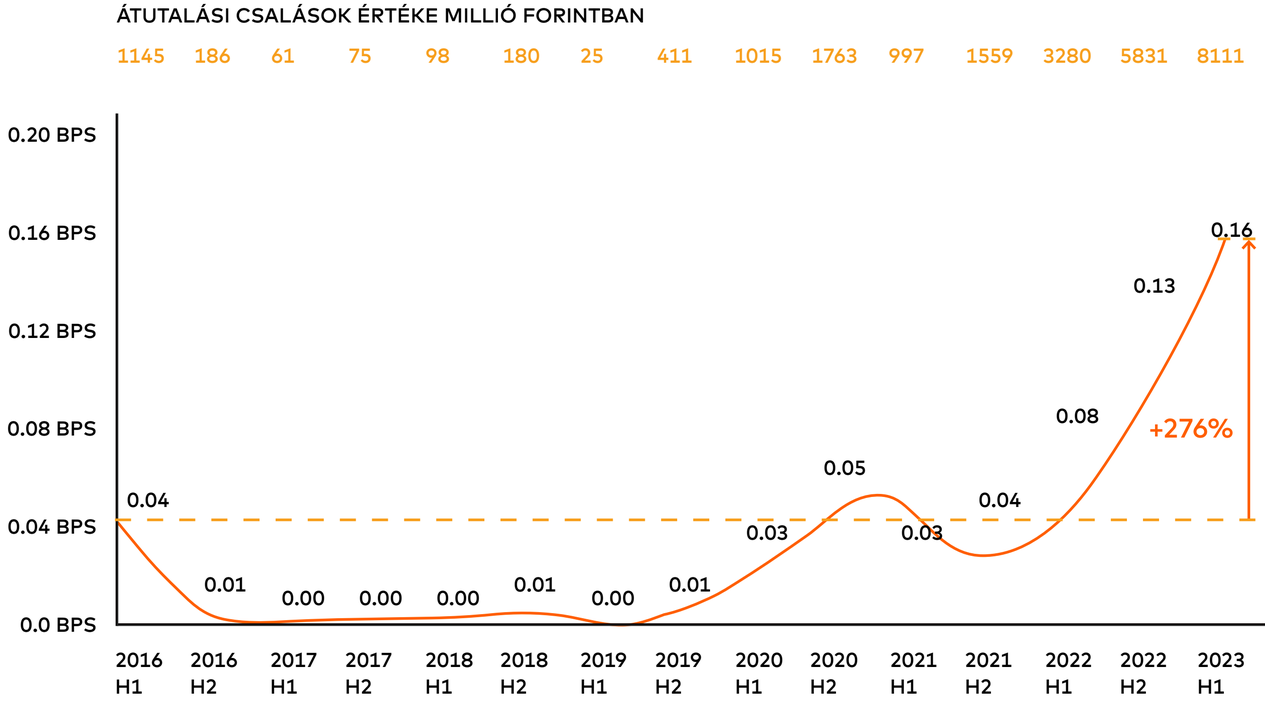
A kártyás, készpénzfelvételi és **AZ ÁTUTALÁSSAL KAPCSOLATOS CSALÁSOK** közül az utóbbi a **LEGALACSONYABB** az Európai Gazdasági Térségben - mind a fizetési érték, mind a volumen tekintetében. 2020-ban az átutalási csalás a fizetések értékében 0,03 és 0,25 bázispont között mozgott, a medián értéke 0,1 bázispont volt. **MAGYARORSZÁGON ÉS MÁS KELET-KÖZÉP-EURÓPAI ORSZÁGOKBAN** tapasztalt csalási arányok átlagosan **A NYUGAT-EURÓPAI** csalások mindössze **EGYÖTÖDÉNEK** feleltek meg.

Az **ELEKTRONIKUS ÚTON** - azaz bármely elektronikus platformon keresztül - **KEZDEMÉNYEZETT** fizetéseknél az átutalási csalások aránya **HÁROMSZOR MAGASABB** volt, mint a nem elektronikus úton kezdeményezetteknél. A kártyás csalásokra ez fordítottan igaz: a **CSALÁSNAK LEGINKÁBB KITETT** fizetések *(kibocsátói és elfogadói oldalról egyaránt)* nem elektronikusan kezdeményezettek voltak. A **NEM ELEKTRONIKUS ÚTON KEZDEMÉNYEZETT** kártyás fizetések négyszer nagyobb valószínűséggel voltak csalásban érintettek.

A nem távoli - azaz nem interneten vagy távközlési eszközökön keresztül végrehajtott - átutalások esetében az **ERŐS ÜGYFÉL-HITELESÍTÉS** *(SCA[1])* **ÁLTAL VÉDETT ÁTUTALÁSOK** csalási aránya **FELE AKKORA** volt, **MINT AZ SCA NÉLKÜL HITELESÍTETT ÁTUTALÁSOKÉ.** A távoli átutalásokon belül ez fordítottan igaz. **AZ SCA-VAL HITELESÍTETT ÁTUTALÁSOK** csalási aránya majdnem tízszer nagyobb volt, mint az SCA-val nem védett átutalásoké, ami valószínűleg az SCA-fizetések magasabb kockázati tényezőjének köszönhető. Például az **SCA-VAL VÉDETT FIZETÉSEK** nagyobb valószínűséggel vannak kitéve a csalók részéről a **PSZICHOLÓGIAI MANIPULÁCIÓ** *(social engineering)* egy formájának, és így nagyobb kockázatot jelentenek

Forrás(ok): Európai Banki Hatóság

MAGYARORSZÁG: AZ ÁTUTALÁSI CSALÁSOK ARÁNYA ÉS ÉRTÉKE JELENTŐSEN MEGUGROTT AZ ELMÚLT KÉT ÉVBEN



2016 második felétől 2019-ig az éves átutalási csalások szintje 1000 millió forint alatt volt. **2020 MÁSODIK FELÉRE AZONBAN A DIGITALIZÁCIÓ NÖVEKEDÉSÉVEL EZ A SZÁM 1700 MILLIÓ FORINT FÖLÉ SZÖKÖTT.**

2023 első felére több mint **8 MILLIÁRD FORINTOT ÉS 0,16 BÁZISPONTOT ÉRT EL** az átutalási csalások nagysága Magyarországon. A kártyacsalásokhoz képest az átutalási csalások bázispontban kifejezve alacsonyabbak, de forintértékben kifejezve magasabbak.

ÁTUTALÁSI CSALÁSOK ARÁNYA ÉS ÉRTÉKE AZ ELEKTRONIKUS FIZETÉSEKNÉL MAGYARORSZÁGON
(2016 H1 – 2023 H1) (BÁZISPONT, MILLIÓ FORINT)

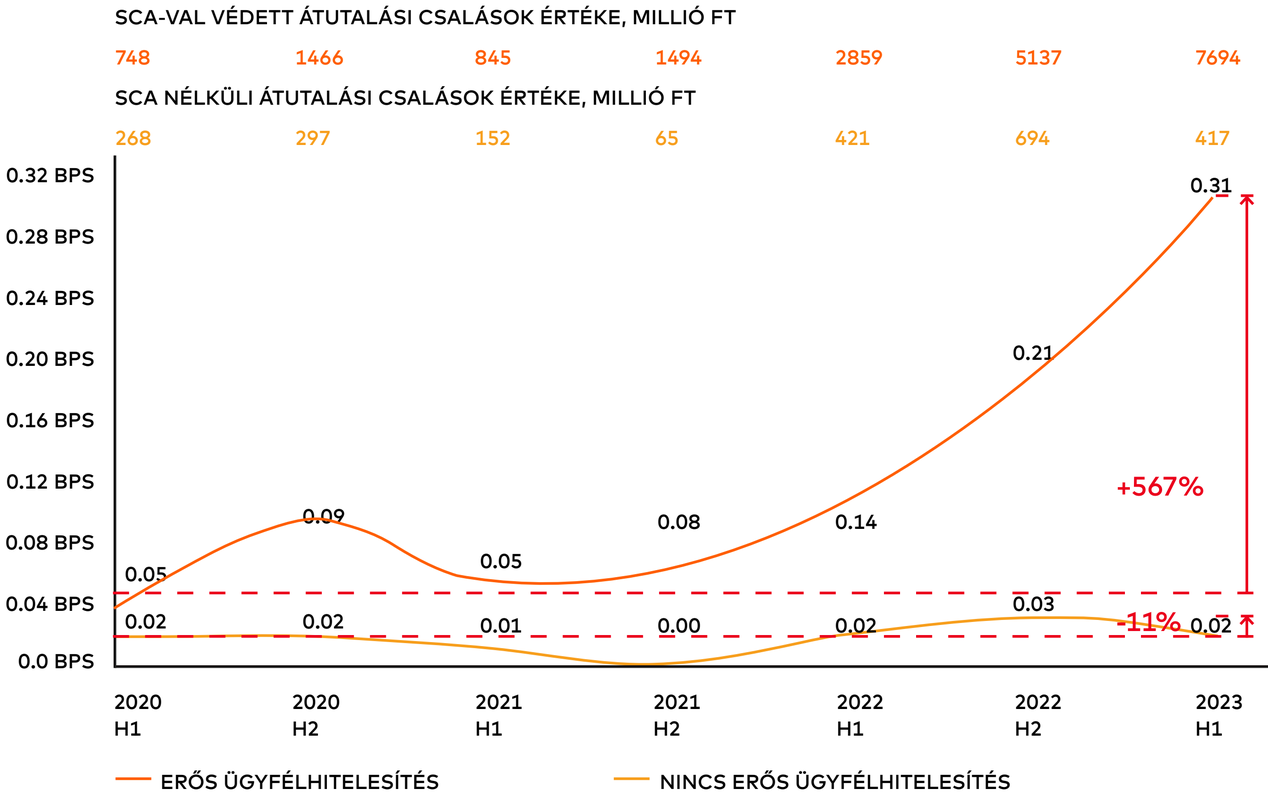
Forrás(ok): Magyar Nemzeti Bank(II.1; II.1c; III.8; III.9b)

AZ SCA-VAL TÖRTÉNŐ TRANZAKCIÓKAT
A PSZICHOLÓGIAI MANIPULÁCIÓ MIATT A CSALÁS NAGYMÉRTÉKBEN ÉRINTI

A kártyákhoz hasonlóan a felhasználók is az SCA használata felé mozdultak el, **ÍGY A CSALÓK IS.**[1]

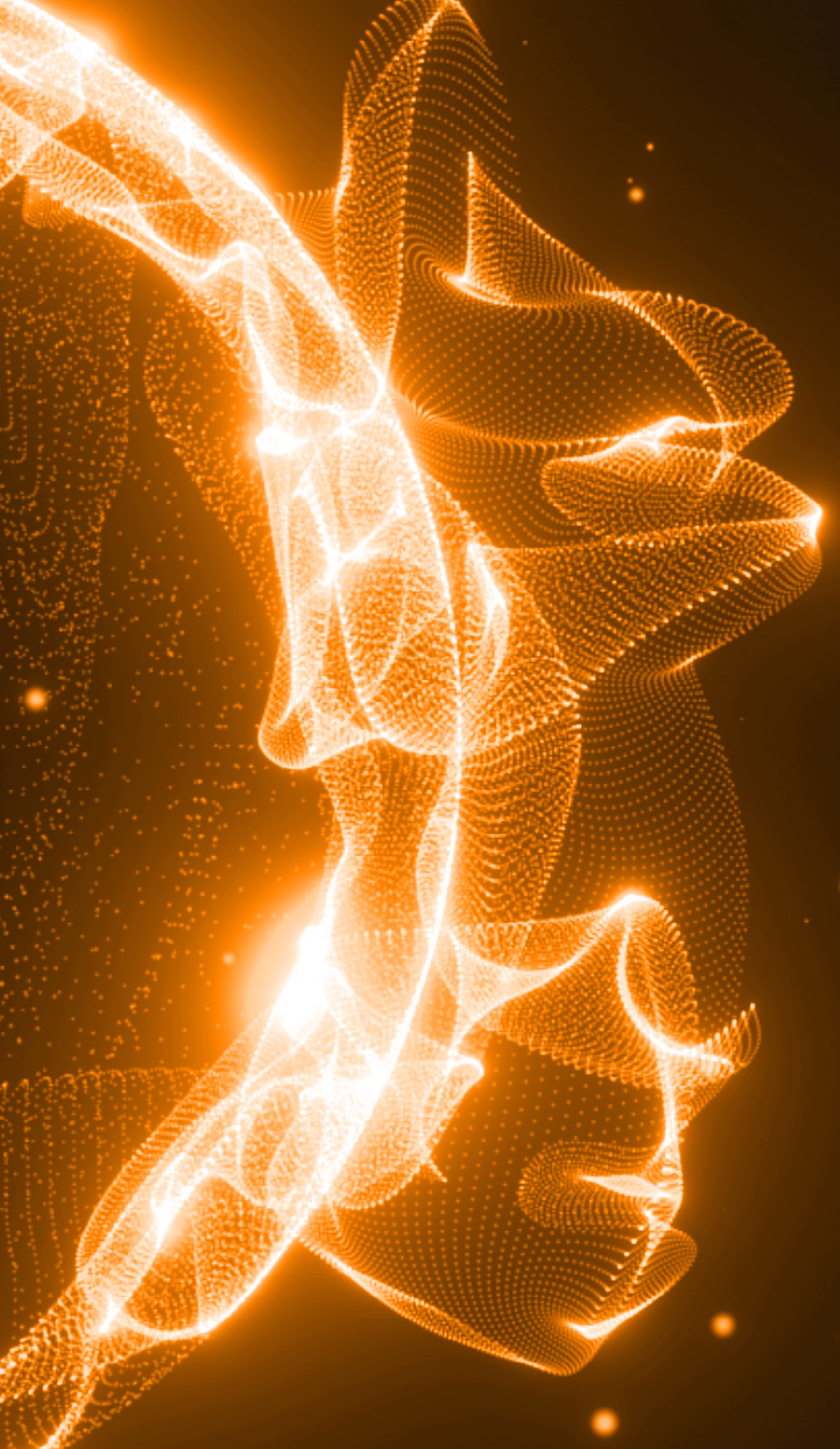
A csaló SCA-tranzakciók a 2020 első félévi közel 750 millió forintról több mint 7,5 milliárd forintra nőttek 2023 első félévére, és ugyanezen időszak alatt 0,05 bázispontról 0,31 bázispontra emelkedtek. Az SCA nélküli tranzakciók több mint 2 évig 0,02 bázispont körüli csalási rátán maradtak, és 2022 második felében érték el csak a 0,03 bázispontot.

Az EU-hoz hasonlóan ez a tendencia is világosan mutatja, hogy bár az SCA fokozott biztonságot nyújt a jogosulatlan csalások ellen, **KORLÁTOZOTT VÉDELMET NYÚJT, A CSALÓKKAL SZEMBEN AKIK PSZICHOLÓGIAI MANIPULÁCIÓ KÜLÖNBÖZŐ FORMÁIT HASZNÁLJÁK** a felhasználók bizalmának elnyerésére és arra, hogy rávegyék őket a hamis tranzakciók hitelesítésére.



ÁTUTALÁSI CSALÁSOK ÉRTÉKE ÉS ARÁNYA AZ ELEKTRONIKUS FIZETÉSEKNÉL SCA-VALÉS ANÉLKÜL MAGYARORSZÁGON
(2020 H1 – 2022 H1) (BÁZISPONT, MILLIÓ FORINT)

Forrás(ok): Magyar Nemzeti Bank(II.1; II.1c; III.8; III.9b)
1) 2021 Jan. 1 volt a határidő a magyar bankoknak hogy bekapcsolják az SCA-t



A CSALÓK A JOGOSULT VISSZAÉLÉSEK FELÉ FORDULNAK, HOGY KIHASZNÁLJÁK A HOMO DIGITALIS GYENGESÉGÉT, HISZEN

AZ INFRASTRUKTÚRA SOKKAL VÉDETTEBB

Ahogy a szabályozási törekvések és az SCA-hoz hasonló védelmi mechanizmusok hatályba léptek, a csalók olyan felhatalmazott csalásokat kezdtek alkalmazni, amelyek megkerülték ezeket a védelmi szinteket. Ezt tovább segíti a digitalizáció növekvő szintje, amely lehetővé teszi az információk és az infrastruktúra alacsony költségű és gyors elérhetőségét az ilyen támadások megkönnyítése szempontjából. Például a minimális technikai ismeretekkel rendelkező csalók a dark weben keresztül könnyen bérelhetnek olyan személyzettel rendelkező ügyfélszolgálatot, akik végrehajtják a támadásokat. A nagyszabású csalások felállításához nagyon csekély speciális ismeretekre van szükség.

MAGYAR PÉLDA:
2021-ben a rendőrség letartóztatott egy Dominikai Köztársaságban élő férfit, aki egy magyarországi ingatlancsalási rendszer vezetője volt. Áldozatait azzal hitegette, hogy törvényes ingatlanvásárlást vagy -bérlést végeznek. Több, asszisztensként vagy ügyvédként fellépő alkalmazottat használt, hogy az ügyletek valósnak tűnjenek. Miközben Dél-Amerikából koordinálta a rendszert, sok alkalmazottja nem volt tudatában annak, hogy illegális tevékenységet folytat.

Forrás(ok): Mastercard, Police.hu

A KIBERBIZTONSÁG

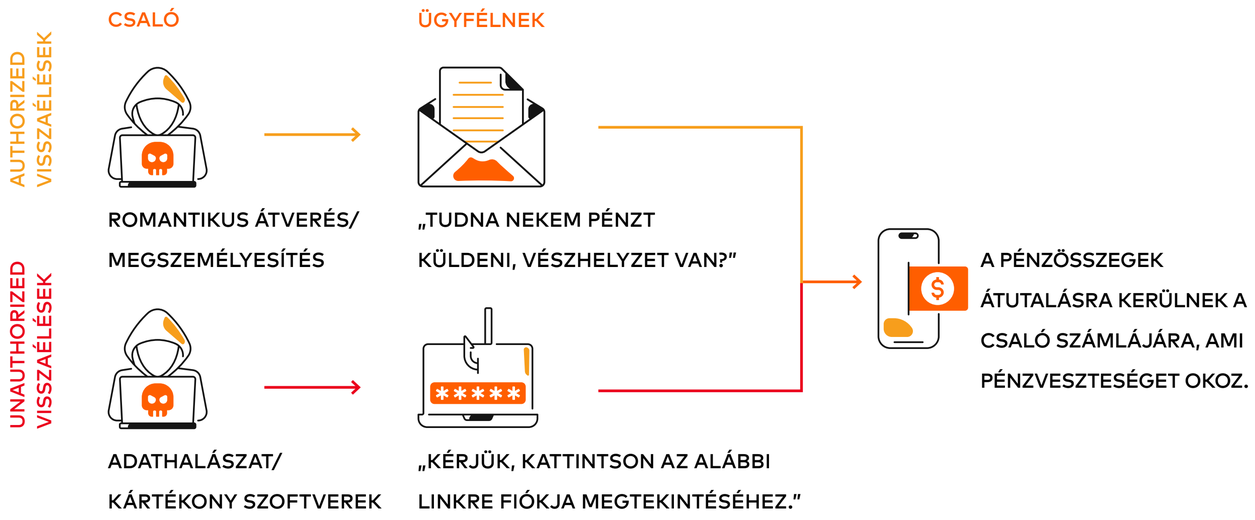
FŐ KIHÍVÁSAINAK KEZELÉSE

KORMÁNYOK,
SZERVEZETEK ÉS
VÁLLALATOK ÁLLNAK
A KIBERTÁMADÁSOK
FRONTVONALÁN

A FIZETÉSI CSALÁSOK A FELHASZNÁLÓK ÁLTAL ENGEDÉLYEZETT, AZAZ AUTHORIZED, ILLETVE UNAUTHORIZED CSALÁSOKRA OSZTHATÓK.

AUTHORIZED VISSZAÉLÉSEK:
A csalók az **E-MAILES PSZICHOLÓGIAI MANIPULÁCIÓ KÜLÖNBÖZŐ TÍPUSAIT HASZNÁLJÁK A FELHASZNÁLÓK BIZALMÁNAK ELNYERÉSÉRE,** amikor SMS-ben, e-mailben vagy telefonon lépnek kapcsolatba az ügyfelekkel, és úgy tesznek, mintha egy megbízható szervezetet képviselnének. Az ügyfél bizalmának elnyerése lehetővé teszi a csalók számára, hogy manipulálják az ügyfelet, hogy tranzakciókat kezdeményezzen vagy megváltoztassa a fizetési adatait *(pl. e-banking)*.

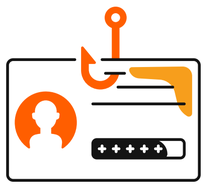
UNAUTHORIZED VISSZAÉLÉSEK:
A csalók **KIFINOMULT ADATHALÁSZAT ÉS KÁRTÉKONY SZOFTVEREK** segítségével megszerzik a felhasználó hitelesítési adatait, hogy birtokukba vehessék a felhasználói fiókot, és így a csalók átutalhassanak pénzt az irányításuk alatt álló számlákra.



Forrás(ok): Mastercard, Police.hu

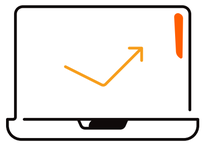
ÖT FŐ TREND,

AMELY A MODERNKORI FIZETÉSI CSALÁSOKAT FORMÁLJA:



SZEMÉLYAZONOSSÁGI LOPÁSOK

A SZEMÉLYAZONOSSÁG IGAZOLÁSA ÉS AZ ONLINE HITELESÍTÉSI FOLYAMATOK alapvető szükségletté válnak a személyazonosság-lopás elleni küzdelemben.

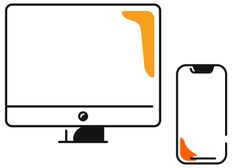


VÁLTOZÓ MAKROGAZDASÁGI KÖRÜLMÉNYEK

AZ ÜZLETI KÖRNYEZET BIZONYTALANSÁGA - például a COVID-19 és az ukrajnai háború - beépül a csalási taktikákba, ami nagyobb sebezhetőséget eredményez.

KÖVETKEZŐ GENERÁCIÓS FIÓKÁTVÉTELEK

A pszichológiai befolyásolás és az adatlopás kifinomult formáinak megjelenésével az ügyfelek személyes adatai egyre nagyobb veszélynek vannak kitéve.



FOKOZOTT KÖZÖSSÉGI MÉDIA HASZNÁLAT

A közösségi média gyakori eszköz mind **BEFEKTETÉSI, ROMANTIKUS CSALÁSOKRA** és pénzmosásra. Az interneten eltöltött idő növekedésével, a közösségi médiás csalásokra való fogékonyság is emelkedik.

FEJLŐDŐ FIZETÉSI TECHNOLÓGIÁK

A BUY NOW PAY LATER fiókokat és a kriptopénz fizetéseket gyakran használják a fizetési csalások során a kevésbé rigorózus szabályozás miatt

Forrás(ok): Juniper Research

A LEGGYAKORIBB FIZETÉSI CSALÁSOK EURÓPÁBAN:

SOCIAL ENGINEERING, SZEMÉLYAZONOSSÁG-LOPÁS, KÁRTYATESZTELÉS

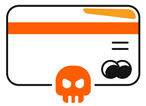
A CSALÁSI TÁMADÁSOK FŐ TÍPUSAI

PHISHING: olyan támadási típusokra utal, amelyek során a csalók az áldozatok személyes adataihoz, például hitelkártyaadatokhoz való hozzáféréssel próbálnak pénzt lopni.

WHALING: *(más néven CEO csalás)* egy szervezeten belüli magas pozíciójú egyének megszemélyesítésével gyakorlonak nyomást a csalók az alkalmazottakra, hogy adják meg adataikat.

PHARMING: egy másik vezető támadástípus, amelyben a csalók célja az online vásárlók átirányítása egy hamis weboldalra.

SZEMÉLYAZONOSSÁG-LOPÁS: a social engineering egyik lehetséges következménye. Ennél a támadási módszernél az ügyfelek adatait ellopják és csalásra használják fel.



KÁRTYATESZTELÉS: olyan csalási tevékenységet foglal magában, amelynek során az elkövetők a kártyacsalás vagy a kártyaadatok tovább-értékesítése előtt megállapítják az ellopott kártyaadatok érvényességét, illetve a pénzeszközök rendelkezésre állását.

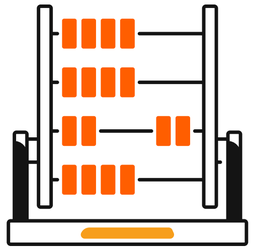
Amerikában a kártyatesztelés a kereskedők által leggyakrabban tapasztalt támadási módszer. Észak-Amerikában - más földrajzi területekkel ellentétben – a first-party csalás is széles körben elterjedt. Ez a támadástípus személyazonosság-lopás nélkül történik; maguk a csalók azok, akiknek a számláit csaláshoz használják, az áldozatok vagy harmadik felek bevonása nélkül.

Forrás(ok): Juniper Research

KÁRTYAELFOGADÓK HATÁSOSAN AKARJÁK KEZELNI A CSALÁSOKAT,

ÖT KIHÍVÁSSAL KELL SZEMBENÉZNIÜK

A CSALÁS HÁLÓZAT- SZINTŰ ÁTTEKINTÉSÉNEK HIÁNYA



HATÉKONYTALAN ÉS NEM MEGFELELŐ JELENTÉSI FOLYAMATOK

A „MONEY MULING" TÉRNYERÉSE

KORSZERŰTLEN CSALÁSKEZELÉSI RENDSZEREK

A CSALÁSSAL KAPCSOLATOS TUDATOSSÁG HIÁNYA

Forrás(ok): Mastercard Advisors Analysis

A FIZETÉSEKET ÉRINTŐ CSALÁSOK KIHÍVÁSAI:

A CSALÁS HÁLÓZAT-SZINTŰ ÁTTEKINTÉSÉNEK HIÁNYA

HOGY TÖRTÉNNEK A TÁMADÁSOK?

- A legtöbb pénzintézet nem rendelkezik a **HÁLÓZATI SZINTŰ ÁTTEKINTÉSHEZ ÉS A BANKOK KÖZÖTTI KOMMUNIKÁCIÓHOZ** szükséges technológiával: ennek következtében a bankok többsége csak a saját tranzakcióihoz fér hozzá, és nem tudja követni a hatáskörén kívül eső csalárd tranzakciókat. A csalárd tranzakciót követően a csalók elsődleges célja a nyomon követhetőség csökkentése azáltal, hogy a megszerzett pénzösszegeket a lehető leggyorsabban, több tranzakció révén különböző bankoknál vezetett különböző számlákra juttatják el.

MIT TEHETÜNK ELLENE?

- Ahhoz, hogy a bankok hatékonyan azonosíthassák a csalásokat és reagálhassanak rájuk, olyan rendszerrel kell rendelkezniük, amely megkönnyíti a több pénzügyi intézmény közötti kommunikációt. Egy ilyen rendszer lehetővé teszi a csalás által érintett valamennyi szereplő számára, hogy közösen használják ki csaláskezelő rendszereiket, kövessék nyomon a pénzeszközöket és térítsék meg az áldozatok kárát.

MILYEN LÉPÉSEKET TEHETÜNK A MEGELŐZÉS FELÉ?

- A pénzintézeteknek **1) OLYAN MEGOLDÁSOKAT KELL BEVEZETNIÜK, AMELYEK LEHETŐVÉ TESZIK SZÁMUKRA A CSALÁSOK HÁLÓZATI SZINTŰ ÁTTEKINTÉSÉT,** az egyetlen félre vonatkozó nézet helyett; és **2) MEG KELL TANULNIUK A TÖBBI INTÉZMÉNNYEL VALÓ, FELEK KÖZÖTTI KOMMUNIKÁCIÓT** a csaláskezelési technikák közös kihasználása érdekében.

"A bankoknak közösen kell dolgozniuk a riportálási és vizsgálati folyamataik egységesítésén ahhoz, hogy változást érjenek el. Ma az a helyzet, hogy a fizetési csalások során ellopott pénzek számos esetben már egy-két órán belül lenyomozhatatlanná válnak, mivel többször, gyorsan egyik számláról a másikra utalják őket."

DANIEL WITTINGHOFF
Director
Cyber Business Development
Mastercard

Forrás(ok): Mastercard Advisors Analysis

A FIZETÉSEKET ÉRINTŐ CSALÁSOK KIHÍVÁSAI:

HATÉKONYTALAN

ÉS NEM MEGFELELŐ JELENTÉSI FOLYAMATOK

HOGY TÖRTÉNNEK A TÁMADÁSOK?

- Nincs egyetlen olyan átfogó jelentési rendszer, amely lehetővé tenné a pénzforgalmi szolgáltatók és a pénzintézetek számára a fizetési csalások nyomon követését, jelentését és elemzését. Ráadásul a legtöbb pénzintézet lassú csalás-felderítési mechanizmusokkal rendelkezik, ami tovább nehezíti a csalások bejelentését.
- Ennek eredményeképpen a pénzügyi ökoszisztéma szereplői **KÜLÖNBÖZŐ MEGKÖZELÍTÉSEKET ALKALMAZNAK A CSALÁSOK BEJELENTÉSÉRE, AMI MEGNEHEZÍTI A KORÁBBI CSALÁSI ESETEKBŐL VALÓ HELYES KÖVETKEZTETÉSEK LEVONÁSÁT** és a jövőbeli csalások mérséklését.

MIT TEHETÜNK ELLENE?

- A pénzügyi ökoszisztéma szereplőinek egységes módon kell racionalizálniuk jelentéstételi gyakorlatukat.

MILYEN LÉPÉSEKET TEHETÜNK A MEGELŐZÉS FELÉ?

- Minden érdekelt félnek hatékony és aktuális csaláskezelési megoldásokkal kell rendelkeznie.
- Biztosítaniuk kell, hogy az egyes szereplők belső rendszerébe integrált megoldások ugyanazokon a jelentéstételi elveken alapuljanak.

"A pénzforgalmi szolgáltatóknak olyan valós idejű tranzakciófigyelő rendszereket kell bevezetniük, amelyek az ügyfél tranzakciós és digitális fizetési szokásai alapján képesek értékelni az egyes tranzakciók kockázatát. Ez lehetővé teszi az időben történő megelőzést még akkor is, ha az ügyfelet korábban már átverték, de a fizetés még nem történt meg. Az elektronikus fizetések elfogadásának biztosítása érdekében kiemelkedő jelentőségű az "Ismerd meg az ügyfeled" elvének magasabb szintű érvényesítése. Hasonlóképpen elengedhetetlen azoknak a mule account-oknak az azonosítása is, amelyek hozzájárulnak a csalások során megszerzett összegek gyors eltűnéséhez. Ebben az esetben ismételten kiemelhetjük a tranzakciós szokások nyomon követésének és az ügyfélprofilok készítésének fontosságát."

LUSPAY MIKLÓS
Pénzügyi infrastruktúrák igazgatóság vezetője
MNB

Forrás(ok): Mastercard Advisors Analysis

A FIZETÉSEKET ÉRINTŐ CSALÁSOK KIHÍVÁSAI:

A „MONEY MULING” TÉRNYERÉSE

HOGY TÖRTÉNNEK A TÁMADÁSOK?

- A pénzfutárok olyan személyek, akik - gyakran díj ellenében - **CSALÓK MEGBÍZÁSÁBÓL ILLEGÁLISAN SZERZETT PÉNZESZKÖZÖKET UTALNAK ÁT,** akiknek személyazonosságát és tartózkodási helyét így nehezebb felderíteni. A lopott pénzeszközök átvételekor a futtatóknak ki kell venniük vagy át kell utalniuk a pénzeszközöket egy másik számlára. E csalások nagy része határokon átnyúló tranzakciókat foglal magában, amelyek során a futtatók **KÜLFÖLDI SZÁMLÁKRA UTALNAK ÁT PÉNZESZKÖZÖKET.**
- A pénzcsalás súlyossága ellenére a legtöbb futtató nincs tisztában a fizetési csalásban játszott szerepével. A pénzcsempészeket gyakran online csalásokon keresztül toborozzák törvényesnek tűnő állásokra.

MIT TEHETÜNK ELLENE?

- A csaláskezelés egyik legfontosabb prioritása a csaló-számlák azonosítása.

MILYEN LÉPÉSEKET TEHETÜNK A MEGELŐZÉS FELÉ?

- A pénzcsalók felderítésére szolgáló reaktív csalási megoldások bevezetése mellett **A SZERVEZETEKNEK FEL KELL ISMERNIÜK A PÉNZMOSÁS ELLENI (AML) SZABÁLYOZÁSOK ÉS ELJÁRÁSOK FONTOSSÁGÁT.**

Forrás(ok): Mastercard Advisors Analysis

A FIZETÉSEKET ÉRINTŐ CSALÁSOK KIHÍVÁSAI:

KORSZERŰTLEN

CSALÁSKEZELÉSI RENDSZEREK

HOGY TÖRTÉNNEK A TÁMADÁSOK?

- A fizetési ökoszisztéma egyre több szereplője számára jelent kihívást, hogy naprakész maradjon az új csalásmegelőzési rendszerekkel, valamint a fizetési csalásokat érintő jogszabályi vagy szabályozási változásokkal kapcsolatban, ami jelentős akadályt jelent a csalásmegelőzésben.

MIT TEHETÜNK ELLENE?

- A szervezeteknek - bankoknak, kereskedőknek és kibocsátóknak egyaránt - meg kell érteniük, hogy **EGYETLEN CSALÁSKEZELŐ RENDSZER SEM ELÉG KIFINOMULT AHHOZ, HOGY ELLENÁLLJON A MAI CSALÁSI TAKTIKÁKNAK.** A csaláskezelés különböző típusaihoz különböző megoldások működnek.

MILYEN LÉPÉSEKET TEHETÜNK A MEGELŐZÉS FELÉ?

- A **REAKTÍV RENDSZEREK** segítenek a szervezeteknek az ellopott pénzeszközök utólagos nyomon követésében, így lehetővé teszik számukra az ellopott pénzeszközök nyomon követését, az áldozatok kártalanítását és a múltbeli támadásokból való tanulást.
- A **PROAKTÍV RENDSZEREK** másrészt kiegészítik a szervezet csaláskockázat-kezelési folyamatait azáltal, hogy előzetes betekintést nyújtanak a csalás által valószínűleg érintett tranzakciókba és/vagy felekbe. A csalás elleni átfogó védelemhez többszintű, különböző belső és külső rendszereket alkalmazó megközelítésre van szükség.

"Egyetlen csaláskezelési rendszer sem elég jó önmagában. A szervezeteknek mindenütt különböző védelmi rétegeket kell továbbra is beépíteniük a csaláskezelési megoldásaikba a csalások hatékony kezelése érdekében."

RICHARD LUFF
Vice President of Product Development, Mastercard

Forrás(ok): Mastercard Advisors Analysis

A FIZETÉSEKET ÉRINTŐ CSALÁSOK KIHÍVÁSAI:

A CSALÁSSAL KAPCSOLATOS TUDATOSSÁG HIÁNYA

HOGY TÖRTÉNNEK A TÁMADÁSOK?

- A csalások egyre kevésbé kapcsolódnak közvetlenül a fizetési forgalomhoz, ami azt jelenti, hogy már nem használják ki a fizetési infrastruktúra hiányosságait. Ennek eredményeképpen a fizetési folyamatban való azonosításuk egyre nehezebb feladatot jelent minden érintett fél számára. Ráadásul az ügyfelek nem tudnak lépést tartani a digitalizáció gyors fejlődésével a pénzügyi tudatosság és a kiberbiztonság tekintetében.

MIT TEHETÜNK ELLENE?

- Azzal, hogy befektetnek az érdekelt felek - mind a belső *(pl. alkalmazottak)*, mind a külső *(pl. beszállítók)* - oktatásába, hogy hogyan ismerjék fel a csalást és hogyan reagáljanak rá, a szervezetek **BIZTONSÁGOSABB MUNKAKÖRNYEZETET TEREMTHETNEK,** és a csalási veszteségek csökkentése révén **MEGVÉDHETIK A PROFITJUKAT IS.**

MILYEN LÉPÉSEKET TEHETÜNK A MEGELŐZÉS FELÉ?

- A csalási tudatosság javítása érdekében a szervezeteknek prioritásként kell kezelniük, hogy ne csak betartsák, hanem **NAPRAKÉSZEK IS LEGYENEK A FIZETÉSI CSALÁSOKRA VONATKOZÓ TÖRVÉNYEKET ÉS RENDELETEKET ILLETŐEN.**
- A nagyszabású országos kampányok szintén kulcsfontosságú szerepet játszanak a fizetési csalások megelőzésében és visszaszorításában. Magyarországon a Magyar Bankszövetséggel együttműködve a Magyar Nemzeti Bank országos fogyasztói tudatosságnövelő kampányt indított a kiberbiztonság és a pénzügyi tudatosság témakörében.

Forrás(ok): Mastercard Advisors Analysis

"A bűnözök ezt a hiányosságot kihasználva próbálkoznak olyan módszerekkel, amelyek a kecsegtető ajánlatok vagy éppen a nyomásgyakorlás útján könnyen célba találnak. Gondoljunk csak például fiktív befektetésekre és nyereményjátékokra, a különböző érzelmi zsarolásokra vagy a színlelt visszaélések megakadályozásának felkínálásához kapcsolódó adatszerzésekre. Mindezekre tekintettel az egyik legnagyobb kihívást abban látjuk, hogy elérjük a fogyasztók egységes szintű felkészítését ezen kockázatokkal szemben, mert ők az első védvonal."

BARTHA LAJOS
Pénzügyi infrastruktúrákért és bankműveletekért felelős ügyvezető igazgató, MNB

"A kiberbiztonsági oktatási kampány célja, hogy a fogyasztókat a lehető legtöbb platformon keresztül folyamatosan emlékeztessük ezekre az üzenetekre, hogy kialakuljon egy olyan szokás, amely segít a fogyasztóknak időben felismerni a megtévesztést és pszichológiai manipulációt alkalmazó csalásokat. Ebben az együttműködésben részt vesz a teljes bankszektor, a kártyatársaságok, a kormánypártok és a nyomozó hatóságok."

VARGA LÓRÁNT
Pénzügyi infrastruktúra és pénzforgalom fejlesztési főosztály vezetője, MNB

HOGYAN SEGÍTHET A MASTERCARD A FIZETÉSI CSALÁSOK ELLENI KÜZDELEMBEN?

MILYEN KONKRÉT MEGOLDÁSI LEHETŐSÉGEK VANNAK?

A CSALÁS HÁLÓZAT- SZINTŰ ÁTTEKINTÉSE

HATÉKONY JELENTÉSI FOLYAMATOK BEVEZETÉSE

A „MONEY MULING" MÉRSÉKLÉSE

A CSALÁSKEZELÉSI RENDSZEREK NAPRAKÉSZEN TARTÁSA

A CSALÁSSAL KAPCSOLATOS TUDATOSSÁG JAVÍTÁSA

EZEN KIHÍVÁSOK LEKÜZDÉSÉRE A MASTERCARD KÉT FŐ TERMÉKKATEGÓRIÁBAN KÍNÁL MEGOLDÁSOKAT:

REAKTÍV (TRACE FINANCIAL CRIME)

A Trace Financial Crime a Mastercard reaktív csaláskezelési megoldásainak vezetője. A termék segít a pénzintézeteknek a bűncselekmények utólagos felderítésében és így növeli az ellopott pénz visszaszerzésének valószínűségét. A Trace Financial Crime a hálózat-szintű információkat - az önálló felhasználói adatok helyett - használva, gépi tanulási *(machine learning)* analitikával párosítva javítja a felhasználók csaláskezelési módszereit azáltal, hogy az ellopott pénz elemzését magasabb szintre emeli.

A termék egy fizetési csalást követően szóródási fákat készít, melyek megmutatják a lopott pénz felek közötti mozgását, hogy pénzintézetek biztonsági rendszerein túl is lehessen követni. A Trace Financial Crime integrált nyomkövetési algoritmusa értesíti a felhasználókat a feltételezett mule account-okról.

MEGELŐZŐ (PREVENT CONSUMER AND CORPORATE FRAUD)

A Prevent termékcsalád egy megelőző csaláskezelési megoldás, amely átutalások előtti szűrési folyamatot alkalmaz. Így a pénzügyi intézetek már a bűncselekmény megtörténte előtt felvehetik a harcot.

Ez a termék gépi tanulást *(machine learning)* és testre szabott analitikát használ a korábbi tranzakciós mintákból való tanuláshoz és így határozza meg a csalással járó tranzakciók valószínűségét.

A Prevent a tranzakció elemzését követően a felhasználók számára pontszámot és hozzá tartozó metaadatokat biztosít, amelyekkel támogatni tudja a tranzakció jóváhagyását vagy elutasítását. Továbbá, a termék bevezetése nem igényel nagyszabású működésbeli változásokat a pénzügyi intézményeken belül.

Forrás(ok): Mastercard Advisors Analysis

FÜGGELÉK

ESETTANULMÁNY:
KIBERBIZTONSÁGI MEGOLDÁSOK

HOGYAN SEGÍTHET A MASTERCARD A KIBERBŰNÖZÉS ELLENI KÜZDELEMBEN?

A NUDETECT ÁTTEKINTÉSE

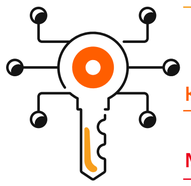
LEÍRÁS

A **NUDETECT** valós idejű védelmet nyújt az online és mobil bankszámlák számára anélkül, hogy megzavarná a felhasználói élményt. Elemzi a felhasználó biometrikus és digitális viselkedését a gyanús bejelentkezési kísérletek és regisztrációk azonosítása érdekében. Az e-kereskedők és a pénzügyi szektor számára is elérhető egy verzió.

FŐBB ELŐNYÖK

FELHASZNÁLÓI ÉLMÉNY JAVÍTÁSA
NÖVELI A BEVÉTELT
CSÖKKENTI A CSALÁSOK SZÁMÁT
CSÖKKENTI A MŰKÖDÉSI KÖLTSÉGEKET

MŰKÖDÉS MÓDJA



A VEVŐ NUDETECT VALÓS IDEJŰ PONTSZÁMA

	MIT TEHET AZ ÜGYFÉL?
ALACSONY/NEM KOCKÁZATOS →	FELESLEGES AKADÁLYOK MEGSZÜNETÉSE MANUÁLIS ELLENŐRZÉS KIKERÜLÉSE TESTRE SZABOTT FELHASZNÁLÓI ÉLMÉNY KIALAKÍTÁSA
KÖZEPES KOCKÁZAT →	EGYEDI AZONOSÍTÁS AUTOMATIZÁLÁSA TOVÁBBI ELLENŐRZÉSHEZ
MAGAS KOCKÁZAT →	MANUÁLIS FELÜLVIZSGÁLAT ELŐÍRÁSA KÉRELEM ELUTASÍTÁSA FELHASZNÁLÓI FIÓK MEGJELÖLÉSE KÉSŐBBI INTERAKCIÓKHOZ

Forrás(ok): Mastercard

ESETTANULMÁNY

HELYZET

Egy régóta működő bank azonosítási megoldása túl sok kényelmetlenséget okozott ügyfeleinek a bejelentkezési élményben. A közel 200 milliárd dolláros eszközállományával rendelkező intézmény úgy vélte, hogy a NuDetect segítségével zökkenőmentes, biztonságos bejelentkezést biztosíthat az ügyfeleinek.

HÁTTÉR ÉS MEGKÖZELÍTÉS

A bank a NuDetect viselkedésalapú biometrikus megoldást építette be a felhasználók bejelentkezéskor történő azonosítására. Egy kéthetes tanulási időszakot követően a szoftver képes volt felismerni a felhasználókat a viselkedésük alapján. A bank forgalmának egy részhalmazából származó, a viselkedésalapú biometrikus megoldással feldolgozott adatok kiértékelése nagy pontosságot mutatott.

EREDMÉNYEK

- **KÖZEL 2,5-SZER TÖBB AZONOSÍTOTT FELHASZNÁLÓ** a bejelentkezéskor, mint a hagyományos eszközalapú és hálózati szintű eszközök használata esetén
- **A FELHASZNÁLÓK 91%-A FELISMERHETŐ** a 14 napos betanulási időszak után
- **0,01%**-os hamis pozitív arány
- Összesen **13 MILLIÓ** vizsgált eset

HOGYAN SEGÍTHET A MASTERCARD A KIBERBŰNÖZÉS ELLENI KÜZDELEMBEN?

A RISKRECON ÁTTEKINTÉSE

LEÍRÁS

A **RISKRECON** egy olyan kiberkockázat-értékelő termék, amelynek célja, hogy az URL-kód elemzésével értékelje, azonosítsa és csökkentse a kiberalapú sebezhetőségeket az ügyfél vállalatának digitális ökoszisztémájában, valamint külsős beszállítók és eladók digitális ökoszisztémájában.

FŐBB ELŐNYÖK

CSÖKKENTI a külső felek kiberkockázatából eredő pénzügyi veszteségeket
NAGYOBB KONTROLL ÉS RUGALMASSÁG a külső felek kiberkockázatának kezelésében
IDŐT ÉS ERŐFORRÁSOKAT TAKARÍT MEG a külső felek kiberkockázatának kezelésében
MEGBÍZHATÓBB & PONTOSABB ÉRTÉKELÉSEKET KÉSZÍT a külső felek kiberkockázatáról

MŰKÖDÉS MÓDJA

1 BIZTONSÁGI FELMÉRÉSEK →

Értékeli a kártevő és zsarolóvírusok elleni küzdelemre irányuló biztonsági intézkedéseket

- Email biztonság
- Behatolási események
- Hálózati szűrés
- DNS biztonság
- Rendszer hírneve

2 INFRASTRUKTÚRA FELMÉRÉSEK →

Felméri a szoftver- és hardverrendszerek kockázatait

- Webes titkosítás
- Alkalmazások biztonsága
- Szoftver javítás
- Rendszer hosting

3 HATÁS-ELEMZÉS →

Elemzi a feltárt problémák hatását azok kritikussága, valamint az adott rendszer érzékenysége alapján

KIBER-KOCKÁZATI MINŐSÍTÉS

ESETTANULMÁNY

HELYZET

Egy nagy globális pénzintézetnek jelentős erőforráshiánnyal kellett értékelnie a külsős felektől származó kiberkockázatokat. A kockázatkezelési csoport minden teljes munkaidős alkalmazottja évente csak néhány tucat külső szolgáltatót tudott értékelni a folyamat összetettsége miatt.

HÁTTÉR ÉS MEGKÖZELÍTÉS

A RiskRecon lehetővé tette a pénzintézet számára, hogy automatizálja a külső szolgáltatók kiberkockázat-értékelését. Mivel csak minimális manuális beavatkozásra volt szükség, a termék segített csökkenteni a pénzintézet erőforrásainak terhelését.

EREDMÉNYEK

10,000+ KÜLSŐ SZOLGÁLTATÓ ELLENŐRZÉSE MINIMÁLIS MANUÁLIS BEAVATKOZÁSSAL

A vizsgálat után a pénzintézet:

- Kockázati kategoriákat és prioritásokat rendelt hozzá külső szolgáltatóihoz
- A precíz adatok kiértékelése után intézkedéseket hozott
- Elindított egy folyamatot a külső szolgáltatók kockázatának nyomon követésére új kiberfenyegetések felmerülésekor

Forrás(ok): Mastercard

HOGYAN SEGÍTHET A MASTERCARD A KIBERBŰNÖZÉS ELLENI KÜZDELEMBEN?

A CYBER QUANT ÁTTEKINTÉSE

LEÍRÁS

A **CYBER QUANT** egy diagnosztikai felmérés alapján – melybe az aktuális fenyegetettségi helyzet be be van építve - értékeli a jelenlegi kiberbiztonsági kockázatokat. A jelenlegi kockázatok és a potenciális veszteségek értékének számszerűsítésével a Cyber Quant támogatja az IT- és biztonsági területekre irányuló beruházások rangsorolását.

FŐBB ELŐNYÖK

KRITIKUS BIZTONSÁGI HIÁNYOSSÁGOK AZONOSÍTÁSA több mint 50 kiberbiztonsági képesség érettségének és fontosságának értékelésével. Szervezetre jellemző **KIBERBIZTONSÁGI KOCKÁZATOK SZÁMSZERŰSÍTÉSE** és a jogsértés potenciális pénzügyi hatásának kiszámítása. **KÖVETKEZŐ LÉPÉSEK RANGSOROLÁSA** a biztonsági helyzet javítása és a kockázat csökkentése érdekében azáltal, hogy szimulációkat végez a legnagyobb megtérüléssel járó intézkedések meghatározásához.

MŰKÖDÉS MÓDJA

A Cyber Quant belülről kifelé irányuló megközelítést alkalmaz a szervezetek kiberbiztonsági kockázatának azonosítására és számszerűsítésére, és szimulációkat futtat a legnagyobb megtérüléssel járó kockázatcsökkentő intézkedések rangsorolása érdekében.

ESETTANULMÁNY

HELYZET

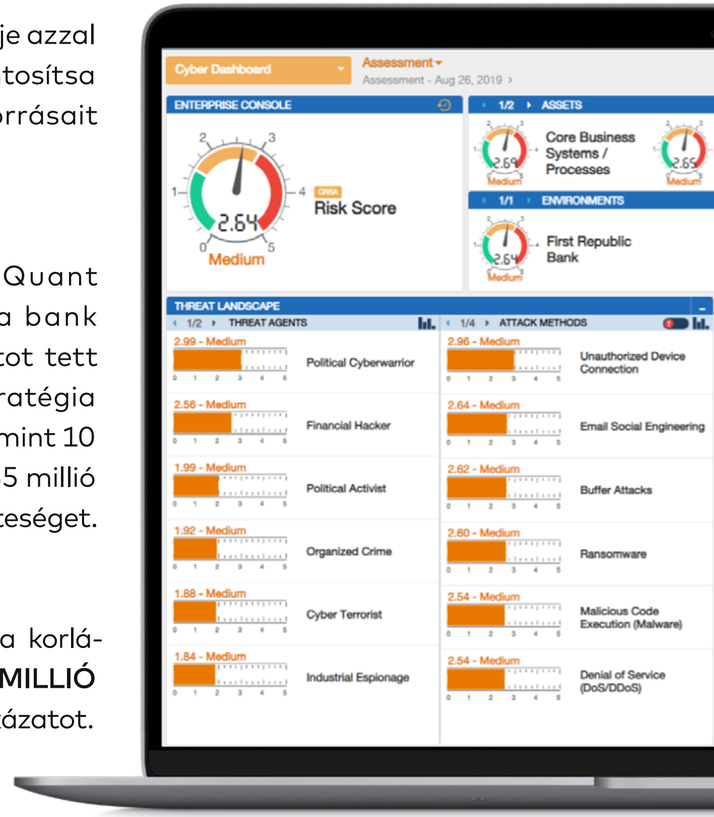
Egy nemzeti bank információbiztonsági vezetője azzal a kihívással szembesült, hogy hogyan összpontosítsa és rangsorolja a szervezet korlátozott erőforrásait a lehető legnagyobb hatás elérése érdekében.

HÁTTÉR ÉS MEGKÖZELÍTÉS

A bank a Mastercarddal közösen Cyber Quant felmérést végzett, amely megvizsgálta a bank jelenlegi kiberbiztonsági helyzetét, és javaslatot tett három priorizált felügyeleti elemre - ez a stratégia lehetővé teszi a bank számára, hogy kevesebb mint 10 millió dolláros kiberbiztonsági beruházással 155 millió dollárral csökkentse a potenciális pénzügyi veszteséget.

EREDMÉNYEK

A projekt eredményeként a bank maximalizálta korlátozott erőforrásainak hatékonyságát, és **155 MILLIÓ DOLLÁRRAL CSÖKKENTETTE** a pénzügyi kockázatot.



Forrás(ok): Mastercard

HOGYAN SEGÍTHET A MASTERCARD A KIBERBŰNÖZÉS ELLENI KÜZDELEMBEN?

A CYBER FRONT ÁTTEKINTÉSE

LEÍRÁS

A **CYBER FRONT** szimulált kiberfenyegetések *(amelyek nem befolyásolják a működő rendszert)* segítségével elemzi a szervezet jelenlegi rendszereit a biztonság folyamatos ellenőrzése, a válaszintézkedések meghatározása és a védekezés javítása érdekében.

FŐBB ELŐNYÖK

ELLENŐRZI, hogy a biztonsági infrastruktúra, a konfigurációs beállítások és a védelmi technológiák rendeltetésszerűen működnek-e.
A meglévő biztonsági infrastruktúra **FOLYAMATOS** tesztelése, anélkül, hogy várni kellene a sebezhetőségi vizsgálati alkalmakra.
A fenyegetések és támadási módok azonosításával megérteni a **FENYEGETÉS VALÓSZÍNŰSÉGÉT.**
BIZTOSÍTANI, HOGY A BIZTONSÁGI MŰVELETI SZEMÉLYZET ÉS AZ INCIDENSRE REAGÁLÓK FELISMERJÉK A TÁMADÁSOKAT, és ennek megfelelően tudjanak reagálni a kiberelhárítási gyakorlatok során.

AMIVEL A CYBER FRONT KITŰNIK

- A Mastercard csapata az ügyféllel közösen a 9000+ egyedi fenyegetésen és 500+ egyedi forgatókönyvön alapuló, folyamatos szimulációs teszteket lehetővé tevő platform létrehozásán dolgozik, ami a kezelendő fenyegetések jobb azonosítását eredményezi.
- A fenyegetések és forgatókönyvek naponta frissülnek
- A tesztelt események és fenyegetések típusai, az eredmények és az ajánlott megoldások egy központi műszerfalon jelennek meg.

Forrás(ok): Mastercard

1 

A Mastercard tanácsadói elemzik a jelenlegi hálózati struktúrát, és útmutatást adnak az optimális Cyber Front telepítési architektúrához.

2 

A rendszer adminisztrátor beveti a szimulációs ügynököket és elindítja az értékeléseket, amelyek perceken belül eredményt adnak, a részletes elemzés pedig órákon belül elkészül.

3 

A Cyber Front a szervezet biztonságtechnológiai szállítóira vonatkozó ajánlásokat ad a Cyber Front széles körben használt technológiák megelőzését szolgáló adatbázisából.

4 

A Mastercard útmutatást nyújt az ajánlások rangsorolásához és végrehajtásához, beleértve a Cyber Quant integrációját is, a kiemelt kockázatok orvoslása érdekében.

5 

A rendszeradminisztrátor végrehajtja az ajánlásokat, míg a Mastercard tanácsadói az azonosított, rangsorolt támadások alapján elkészítik a reagálási forgatókönyveket.

6 

Folyamatos szimulációk mérik a biztonsági helyzet javulását és figyelik az új fenyegetéseket.

ESETTANULMÁNY:

FIZETÉSEKET ÉRINTŐ CSALÁSOK MEGOLDÁSA

HOGYAN SEGÍTHET A MASTERCARD A FIZETÉSI CSALÁSOK ELLENI KÜZDELEMBEN?

A TRACE FINANCIAL CRIME ÁTTEKINTÉSE

LEÍRÁS

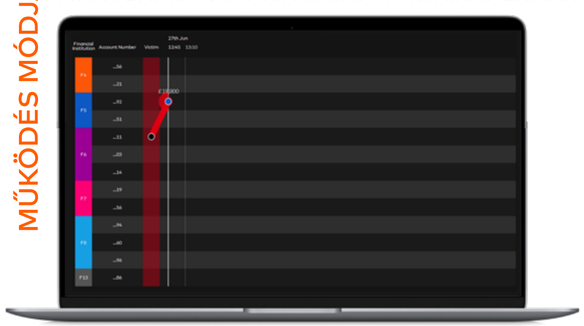
A Trace Financial Crime segít bankoknak és pénzügyi intézményeknek a visszaélések utólagos felderítésében, és így növeli a pénzeszközök visszaszerzésének és az ügyfelek védelmének valószínűségét. A Trace Financial Crime az egyedi felhasználói adatok helyett hálózati szintű betekintést használ, és gépi tanulási elemzésekkel párosítva javítja a felhasználók csaláskezelési taktikáit azáltal, hogy az ellopott pénzeszközök elemzését magasabb szintre terjeszti ki.

FŐBB ELŐNYÖK

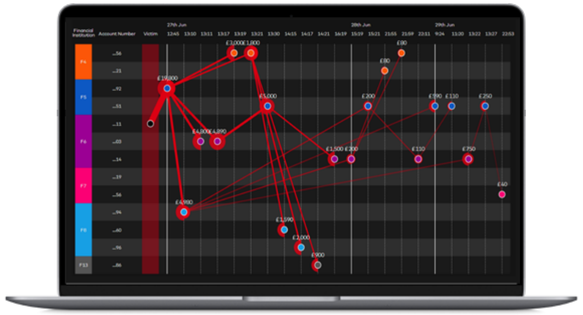
Pénzmosással **GYANÚSÍTOTT SZÁMLÁK AZONOSÍTÁSA**
Szabályozó hatóságok által kiszabott **BÍRSÁGOK ELKERÜLÉSE**
HATÉKONYSÁG és **KÖLTSÉGMEGTAKARÍTÁS** megvalósítása
VÉDI a vállalat **HÍRNEVÉT** és az ügyfelek **VAGYONÁT.**

MŰKÖDÉS MÓDJA

MÍG A BANKOK CSAK A SAJÁT FIÓKJAIKAT LÁTJÁK



TRACE HÁLÓZATI SZINTŰ NÉZETET BIZTOSÍT



ESETTANULMÁNY

HELYZET

Egy bankot értesített egy ügyfél arról, hogy csalás áldozata lett. A csaláshoz kapcsolódó tranzakció részleteit a Trace Financial Crime használatával fedezték fel.

HÁTTÉR ÉS MEGKÖZELÍTÉS

A fiók egy negyedik generációs pénzöszvér fiók volt egy összetett hálózaton belül. A fiók tevékenysége tipikusan pénzöszvér tevékenység volt: nagy mennyiségű pénzeszköz fogadása és gyors kifizetése. A pénzeszközök nagy részét ugyanazon a bankon belül egy másik számlára küldték, amelyről kiderült, hogy nagy mennyiségű pénzeszközöket fogad, és azokat továbbküldi.

EREDMÉNYEK

A nyomozás előrehaladtával egy több mint **70 AKTÍV FIÓKBÓL ÁLLÓ CSALÓHÁLÓZATOT LEPLEZTEK LE ÉS SZÁMOLTAK FEL.**

Forrás(ok): Mastercard

HOGYAN SEGÍTHET A MASTERCARD A FIZETÉSI CSALÁSOK ELLENI KÜZDELEMBEN?

A PREVENT CONSUMER AND CORPORATE FRAUD ÁTTEKINTÉSE

LEÍRÁS

Ez a preventív családkezelési megoldás lehetővé teszi a pénzintézetek számára, hogy a számlák közötti fizetések tranzakció előtti szűrési folyamatának részeként a fizetési csalások ellen felvegye a harcot.

FŐBB ELŐNYÖK

MEGAKADÁLYOZZA az ügyfélveszteségeket
MEGKÜLÖNBÖZTETI ÉS VÉDI az intézmény hírnevét
HATÉKONYSÁG ÉS KÖLTSÉGMEGTAKARÍTÁS létrehozása

MŰKÖDÉS MÓDJA

KÉRELEM
Az előengedélyezett fizetési információ API-n keresztül benyújtásra kerül a Preventnek a fizetés elküldése előtt

PROFILALKOTÁS
Alkalmazott modellek felismerik a gyanús viselkedést

VÁLASZ
Eredmények visszaküldése a pénzügyi intézménynek a valós idejű döntéshozatal támogatása érdekében

DÖNTÉS
A pénzügyi intézmény a Prevent eredményei alapján valós idejű döntést hoz a kifizetésről

FIGYELMEZTETÉS
Fizetés után lekérdezett figyelmeztető jelzések a mélyebb vizsgálathoz

VISSZAJELZÉS
Vizsgálati eredmények visszajelzése API-n keresztül

A CSALÁS VISSZAJELZŐ KÖR FEJLESZTI A GÉPI TANULÁSI MODELLEKET

ESETTANULMÁNY

HELYZET

Egy nagy pénzintézet partnerséget kötött a Mastercarddal annak érdekében, hogy jobban megértsék az átverések hatását a fogyasztói számlaalapú fizetések esetén.

HÁTTÉR ÉS MEGKÖZELÍTÉS

A partnerség eredményeképpen olyan megoldást terveztek és építettek, amely a fogyasztói számlaalapú fizetésekkel kapcsolatos csalások problémáját kezeli. A pozitív eredmények hatására a pénzintézet a Prevent Retail Payment Fraud-ot olyan alapvető változást hozó megoldásként jellemezte, amellyel eddig még nem találkoztak.

EREDMÉNYEK

+50% átlagos többlet mennyiségi felderítési arány a korábban nem észlelt csalásokhoz képest
76% átlagos teljes felderítési arány az összes csalás esetében
21:1 alacsonyabb átlagos hamis pozitív arány, mint a meglévő megoldásoknál

Forrás(ok): Mastercard

KÖSZÖNJÜK!

KERESSEN MINKET:

RACSKÓ TAMÁS

DIRECTOR

PRODUCTS & SOLUTIONS

TAMAS.RACSKO@MASTERCARD.COM

NEMES MÁTÉ

PRODUCT DEVELOPMENT MANAGER

MATE.NEMES@MASTERCARD.COM

GEISZT ROBERT

CONSULTANT

ROBERT.GEISZT@MASTERCARD.COM

WITTINGHOFF DÁNIEL

ÜZLETFEJLESZTÉSI IGAZGATÓ

DANIEL.WITTINGHOFF@MASTERCARD.COM

FORRÁSOK

1. Digital-operational-resilience-act.com: The official website of the DORA initiative https://www.digital-operational-resilience-act.com/
2. European Central Bank: Seventh report on card fraud by the European Central Bank (October 2021) https://www.ecb.europa.eu/pub/pdf/cardfraud/ecb.cardfraudreport202110~cac4c418e8.en.pdf
3. European Banking authority: Discussion Paper on EBA's preliminary observations on selected payment fraud data under PSD2, as reported by the industry (January 2022) https://bit.ly/3TFo5ec
4. European Commission SMEs and Cybercrime 2022 Survey, Ipsos: Flash Eurobarometer - SMEs and Cybercrime (December 2021) https://europa.eu/eurobarometer/surveys/detail/2280
5. Central Bank of Hungary: Fizetési forgalom - II.1, II.1c, II.6, II.6d - (March 2023) https://statisztika.mnb.hu/idosor-1020
6. Central Bank of Hungary: Pénzforgalmi visszaélések - III.2a, III.2b, III.8, III.9b - (March 2023) https://statisztika.mnb.hu/idosor-1024
7. Juniper research: Online Payment Fraud: Market Forcast, Emerging threats & Segment analysis 2022-2027 (July 2022) https://www.juniperresearch.com/researchstore/fintech-payments/online-payment-fraud-research-report
8. Mastercard Cyber Quant platform: Proprietary platform of Mastercard - Data gathered from 14 data sources including: Mastercard threat intelligence, cybersecurity event reports, dark web websites, hacker forums, RSS feeds
9. Merchant savvy: Global Payment Fraud Statistics, Trends & Forecasts (October 2020) https://www.merchantsavvy.co.uk/payment-fraud-statistics/
10. Police.hu: Dominikán vágták le a bűnszervezet csápjait (October 2021) https://www.police.hu/hu/hirek-es-informaciok/legfrissebb-hireink/bunugyek/dominikan-vagtak-le-a-bunszervezet-csapjait
11. Ponemon institute: Data Risk in the Third-Party Ecosystem (October 2022) https://www.riskrecon.com/ponemon-report-data-risk-in-the-third-party-ecosystem-study
12. Prolifics testing: The Most Common Responses To Cyber-Crime In European Countries https://www.prolifics-testing.com/the-most-common-responses-to-cyber-crime-in-european-countries
13. Reuters: Hungary hit by large cyber attack from Asia -Magyar Telekom (September 2020) https://www.reuters.com/article/hungary-cyber-idUKL5N2GN03J
14. Statista 2020: Cyber risk in selected Central and Eastern European (CEE) countries in 2020 (February 2021) https://www.statista.com/statistics/1202279/cee-vulnerability-to-cybercrime/
15. United Nations Office on Drugs and Crime: Estimating illicit financial flows resulting from drug trafficking and other transnational organized crimes (2011) https://www.unodc.org/documents/data-and-analysis/Studies/Illicit_financial_flows_2011_web.pdf
16. EUR-Lex - 32022R2554 - EN - EUR-Lex (europa.eu)
17. European Banking Authority | (europa.eu)