BIOMETRIA és biztonság

1. ALAPVETÉSEK

A biometria a személyek azonosítására szolgáló biztonsági technológia. Elmúltak azonban már azok az idők, amikor egy biztonsági rendszert csak azért vettek meg a vállalatok, mert volt rá költségvetés. Nekünk, biztonsági szakembereknek is fel kellett ismernünk, hogy ha az adott műszaki, biztonsági célt kielégítő rendszer már nem elég jó. Alá kell tudnunk támasztani, hogy megfelelő költség/haszon aránnyal teljesít e. Ezeket a gondolatokat boncolgatjuk cikksoroztunk mai részében.

Mi az a biometria?

Minden szakdolgozat és tanulmány azzal kezdődik, hogy mit is jelent a „biometria" szó. Véleményem szerint kicsit már elcsépelt, de a teljesség kedvéért álljon itt, hátha valaki még nem hallotta. A kifejezés a görög „bio" – élet és „metria" – mérés szavak összeillesztéséből ered. Tehát megmérjük valami élőnek valamilyen jellemzőjét. Legyen ez az élő például az ember, és máris eljutottunk oda, amit napjainkban a személyazonosítás terén biometriának hívunk.

Emberek valamely testi jellemzőjének azonosítása.

Nap, mint nap ezt tesszük a születésünk óta. Először szüleink hangját, illatát és arcát ismerjük fel. Később a rokonainkat, osztálytársainkat, barátainkat is így azonosítjuk. A technika fejlődése azonban csak az elmúlt néhány évtizedben tette lehetővé, hogy automatikus biometrikus felismerő rendszereket készítsünk.

Nézzük meg kicsit részletesebben, mit is jelent pontosan a testi jellemző. Alapvetően minden ember minden jellemzője egyedi. A mi szempontjaink szerint a kérdés csak az, hogy ***ezek adott körülmények között megfelelő költség/haszon mellett azonosíthatók-e***.

Körülménynek tekinthető például a technológiai fejlettség, vagy a genetikai jellemzők adottságai. Például az egyik legpontosabb biometriai jellemzőnk a DNS szekvenciánk. Automatizált felhasználóazonosításra jelen tudásunk szerint mégsem alkalmas, egyrészt mert lassú (bár már hallottunk olyan eszközökről, melyek hozzávetőleg 10 perc alatt tudnak DNS-t azonosítani, ami nagy szó, de mégsem elég gyors) és képzeljük csak el, milyen sorok tudnának kialakulni egy több száz fős beléptetésnél. Másrészről nem tudjuk biztosítani, hogy a DNS-t csak a jogosult felhasználó juttassa az azonosítóba. Egy hajszál, de a számítógépünk billentyűzetére hullott elhalt bőrdarabkáink is alkalmasak a felismerésre.

De mit értünk pontosan költség/haszon arány alatt?

Itt meg kell állnunk egy pillanatra, mert ki kell terjeszteni a gondolatmenetünket a biztonság teljes területére és témánkat ebben az értelmezési tartományban tárgyalnunk. Innen már majd egyszerűen szűkíthetünk a biometria részterületére, hiszen az egy részhalmaza a biztonságnak.

Sajnos nagyon sokszor találkozunk olyan megközelítéssel, hogy a biztonságot önmagában szemlélik, és nem csak felhasználók, hanem szolgáltató szakemberek is. Ha biztonságról esik szó sokszor élőerőre és/vagy technikára gondolunk.

Ennél azonban jóval többről van szó, a biztonság egy igen gyorsan fejlődő tudomány és az emberi aktivitás hátterében mindig ott van még akkor is, ha nem beszélünk róla. Hiszen a biztonság nem egy önmagában létező dolog, mert ha nem lennének katasztrófák, balesetek, emberi hibák és rossz szándékú támadók, akkor nem lenne miről beszélnünk. Egy példával illusztrálva: soha nem szerelnénk zárat az ajtónkra, ha nem lenne vélt vagy valós okunk védekezni az illetéktelen behatolókkal szemben. De szünetmentes tápellátásra sem lenne szükség, ha az áram nem menne el.

Témánk szempontjából tehát az ***emberi tényező*** az egyik kihagyhatatlan faktor.

Ha nagyon leegyszerűsítjük a biztonság kérdését akkor a legfontosabb feladata a ***személyazonosítás*** kell legyen. Gondoljunk csak bele mit valósítunk meg a biztonsági rendszereinkkel:

- a kerítésnek az a feladata, hogy a nem jogosult személyt távol tartsa. Igen ám, de a jogosultnak is be kell jutnia, erre van a kapu. Azon persze a zár, aminek szintén ez a feladata: akinél kulcs van az bejöhet;
- a vagyonvédelmi rendszerek is ezt szolgálják: ha illetéktelen jön be, riasztást kell generálni. A jogosult személy pedig tudja a riasztó kódját vagy van nála jogosult-távirányító;
- a beléptetőrendszer beenged, ha jogosultkártya van nálunk;
- a számlánkon lévő pénzhez a bankkártyánk és a PIN kódunk ismeretében férhetünk hozzá;
- a számítógépünkhöz a jelszavunkkal férhetünk hozzá.

Sok példát lehetne még felhozni, de a lényeg az, hogy az illetéktelen minél kevésbé juthasson be a védett területre, a védett személyhez, értékhez vagy információhoz. A másik fontos tényező az, hogy a jogosult viszont a lehető legkisebb kényelmetlenséggel jusson át a biztonsági rendszereken. Ugye ismerős az, amikor a forgóvillás beléptetőn a vezérigazgató nem húzza le a kártyáját, hanem amikor meglátják az őrök, már messziről nyitják neki a rokkantkaput…

Az embert azonosítjuk és emberekkel szemben védekezünk. Nem utolsó sorban pedig emberek fogják feltenni azt a nem elhanyagolható kérdést: Mennyibe fog ez nekünk kerülni? Mi a ***költsége?*** Talán pongyolább megfogalmazás, de sokkal inkább helyénvaló lenne: Mibe fog ez nekünk fájni? Ugyanis a „költség" nem elsősorban pénzben kifejezhető jellemző. A biztonság mindig kompromisszum eredménye és valaminek a hátrányára születik.

Az első nyilvánvaló gondolat, hogy a pénztárcánk fogja bánni. De például időbe is kerül. A kényelmünk hátrányára nem kevésbé. A memóriánkat is terheli, sőt stresszel is minket. Ezek a hátrányok a ***költségeink***.

Kérem, hogy most szánjanak egy percet arra, hogy végiggondolják, milyen hátrányokkal szembesülünk nap mint nap amikor biztonsági kompromisszumokat hozunk.

Nézzük ezt meg egy egyszerű történeten

keresztül: egynapos külföldi üzleti útra indulunk repülővel.

> ***Reggel felkelünk, lefőzzük a kávénkat, megeszünk egy szendvicset, lezuhanyozunk, majd az összekészített csomagunkkal elindulunk a reptérre. Beszállunk az autónkba és kiautózunk a reptérre. Becsekkolunk és felszállunk a repülőre.***

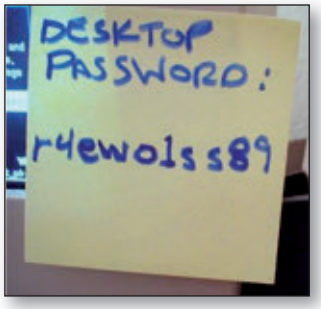
Vizsgáljuk meg költségoldalról ezt a történetet a teljesség igénye nélkül. Jellemzően azokat emeljük ki, amelyek fontosak témánk szempontjából. Félkövérrel az eredeti szöveg olvasható, kapcsos zárójelben dőlt betűkkel a költségeinket, a normál zárójelen belül pedig a költségkategóriákat írtam le:

> **Reggel felkelünk** *[és hatástalanítjuk (kényelem, idő, terhelés) a riasztónk (pénz) éjszakai üzemmódját],* **lefőzzük a kávénkat** *[a jóval drágább biztonsági kávéfőzőnkön (pénz), ami nem fog felrobbanni],* **megeszünk egy szendvicset** *[amihez drágábban vettük meg az alapanyagokat, mert nem tartalmaz „E" összetevőket (pénz, stressz)],* **lezuhanyozunk, majd az összekészített csomagunkkal elindulunk a reptérre** *[bezárjuk a biztonsági ajtót (pénz, idő, kényelem), beriasztunk (memória, stressz), két órával előbb kell kiérnünk (idő, kényelem, stressz)].* **Beszállunk az autónkba** *[nem térnék ki arra, hogy mennyiért vettük az extra védelmi felszereltségű autónkat, kiriasztjuk (pénz), beköjük magunkat (kényelem, pénz – ugye már nem is jut eszünkbe, hogy a biztonsági öv 50 évvel ezelőtt még opcionális felszerelés is alig volt)]* **és kiautózunk a reptérre** *[házi feladat: az úton milyen biztonsági rendszereket használunk?].* **Becsekkolunk** *[Lefóliázzuk a csomagunkat (pénz, idő, kényelem), átmegyünk az ellenőrzésen, fémdetektoron, levesszük a cipőnket (idő, kényelem, stressz)]* **és felszállunk a repülőre**.

Nem szoktunk ezekbe belegondolni, de jelen vannak az életünkben. És talán az is látható, hogy ennek az egyszerű 28 szavas bekezdésnek a teljes elemzése jelentősen meghaladná cikkünk terjedelmi lehetőségeit.

Az is látható, hogy néhány alapvető tényezőn túlmenően mindig az adott cél ismeretében kell meghatározni az ott fontos faktorokat mind költség, mind haszonoldalon.

Nézzünk erre egy példát az IT biztonság területéről. Milyen hosszúságú és bonyolultságú jelszavak megjegyzését várhatjuk el a felhasználóktól? Erről az egy témáról önmagában lehetne egy teljes tanulmányt írni, most csak a példa kedvéért lássunk néhány faktort. Az embereknek egyre több dolgot kell megjegyezniük: PIN kódokat, jelszavakat. A probléma alapvetően ott van, hogy az emberi agy alkalmatlan sok egymással össze nem függő dolog megjegyzésére. Beláthatjuk, hogy egy véletlenszerűen generált jelszó különálló, össze nem függő jelek összessége: g#Hjx5%123. Ezt megjegyezni komoly szellemi teljesítmény. Ezért van az, hogy az emberek általában olyan jelszavakat adnak meg, amelyek egy nagyobb egységként már könnyen megjegyezhetőek: alma (4 karakter, de nem a betűk összességeként gondolunk rá), vagy a születési dátumunk, vagy az irányítószámunk, stb. A számítógépes rendszerekbe történő belépést pedig minden IT biztonsági szakember szeretné minél nehezebben kitalálható vagy feltörhető jelszóval szabályozni. Na de meddig mehetünk el egy jelszó bonyolításában? Mik azok a tényezők, amik ezt felülről korlátozzák? Először is, ha túl bonyolult jelszavakat írunk elő, a frusztrált felhasználók szépen fel fogják írni egy cetlire vagy a billentyűzet aljára. Ismerős ugye?



A másik ilyen tényező, hogy minél bonyolultabb egy jelszópolitika, annál több felhasználói kérés, bejelentés fog az IT osztályra érkezni elfelejtett jelszavak formájában. Csak ezt a két említett tényezőt megvizsgálva beláthatjuk, hogy létezik az a bonyolultsági előírás, ahol már biztonsági rést viszünk be a rendszerbe azáltal, hogy a felhasználók fel fogják írni a jelszavakat, mert nem tudják megjegyezni, illetve az elfelejtett jelszavak miatti munkaidő-kiesés és a támogatás megnövekedett ideje miatti költségnövekedés már nem éri meg a jelszópolitika bonyolítását.

Otti Csaba

A szerző mérnök-közgazdász, magánbiztonsági szakértő, 12 éve többek közt biometrikus, biztonsági és felhasználóazonosító rendszerek tanácsadójaként dolgozik. Ezen időszakban számos nagyvállalat biztonsági koncepciójának elkészítésében vett részt. Az Óbudai Egyetem keretein belül működő Alkalmazott Biometriai Intézet szakmai referense. Biometrikus rendszerekkel kapcsolatos szakmai továbbképzésről további információ a www.abibiometrics.com oldalon található.

■ ***Fenti gondolatmenet összefoglalva:***
A biztonsági megoldásokat mindig egy koncepció keretein belül kell tárgyalni, ahol pontosan meghatározzuk az elérendő célokat, feltárva a kockázatokat, figyelembe véve az emberi tényezőt, a várható költségeket és prognosztizálható hasznokat.

Na és hogy miért fontos a koncepció? Mert nagyon komoly esélye van annak, hogy e nélkül, a sok költségünkhöz veszünk még egy jó adag rejtett kockázatot is.

Ezt a gondolatmenetet analóg módon alkalmazhatjuk és alkalmazzuk is az egyes biometrikus technológiák, megoldások és eszközök vizsgálatánál, elemzésénél.

Talán többeknek úgy tűnhet, hogy ez a cikk valójában nem is kapcsolódik a biometrikus rendszerek témaköréhez. Egyetértek. Mégis sokkal fontosabbnak tartom a szemlélet definiálását mivel ez a nézőpont sokkal tágabb, és a valósághoz közelebb álló, mintha csak eszközökről és paraméterekről beszélnénk. Továbbá ezen elvek mentén fogjuk tárgyalni a biometriát is, így mindenképpen fontos volt az alapvetéseket tisztázni.

Következő cikkünkben a biometria történetét tekintjük át globálisan, illetve az elmúlt 14 évben a magyarországi tapasztalataink alapján. ■