FÜLÖP Árpád – VIRÁG Péter

VÁLLALATI DÖNTÉS EGY ÚJ INFORMÁCIÓBIZTONSÁGI ESZKÖZ, A KVANTUMKULCSCSERE BEVEZETÉSÉRŐL

A szerzők tanulmányukban az információbiztonság egy merőben új, minőségi változást hozó találmányával, a kvantumkulcscserével (QKD-vel – quantum key distribution) foglalkoznak. Céljuk az, hogy az újdonságra mint informatikai biztonsági termékre tekintsenek, és megvizsgálják a bevezetéséről szóló vállalati döntés során felmerülő érveket, ellenérveket. Munkájuk egyaránt műszaki és üzleti szemléletű. Előbb elkülönítik a kvantumkulcscsere hagyományos eljárásokkal szembeni használatának motiváló tényezőit, és megállapítják, milyen körülmények között szükséges a napi működésben alkalmazni. Ezt követően a forgalomban is kapható QKD-termékek tulajdonságait és gyártóit szemügyre véve megfogalmazzák a termék széles körű elterjedésének korlátait. Végül a kvantumkulcscsere-termék bevezetéséről szóló vállalati döntéshozás különböző aspektusait tekintik át. Információbiztonsági és üzleti szempontból összehasonlítják az új, valamint a hagyományosan használt kulcscsereeszközöket. Javaslatot tesznek a védendő információ értékének becslésére, amely a használatbavétel költség-haszon elemzését támaszthatja alá. Ebből levezetve megállapítják, hogy mely szervezetek alkotják a QKD lehetséges célcsoportját. Utolsó lépésként pedig arra keresik a választ, melyik időpont lehet ideális a termék bevezetésére.

Kulcsszavak: **kvantumkulcscsere, információbiztonság, információbiztonsági döntéshozatal, kriptográfiai termékek**

Az adatbiztonság vagy információbiztonság alapvető fontosságú modern világunk információs társadalmában. Az *adatbiztonság* definíció szerint bármely adat jogosulatlan megszerzése, módosítása, tönkretétele elleni védekezéssel foglalkozik, és nem keverendő össze az *adatvédelemmel*, amely az úgynevezett személyes adatok gyűjtésének és felhasználásának korlátozását tartja céljának.

Az információbiztonsági elvek az elektronikus üzletvitel bizonylataira, az elektronikus kereskedelem és kormányzat kommunikációjára egyaránt vonatkoznak. Még általánosabban fogalmazva az elvek kiterjednek minden, elektronikus csatornán történő kommunikáció minden egyes üzenetére.

Az átlagfelhasználó általában maga is elvárja, hogy üzenetei bizalmasak, módosíthatatlanok, törölhetetlenek stb. legyenek, ugyanakkor sokszor nincsen tisztában az ezek elérésére tett műszaki és szervezési erőfeszítésekkel. Ez részben magyarázható azzal, hogy sok funkció már olyan mélyen integrálódott a rendszerekbe, hogy működésük láthatatlan. Egy, az informatikáért felelős vezetőnek viszont mindenképpen helyénvaló ismernie, hogy a szervezetéhez köthető információáramlás során az adatbiztonsági elvek hogyan érvényesülnek még a felszín alatti szinteken is.

Jelen cikk az információbiztonság egy ilyen, mélyen integrálódott elemével, a *kulcscserével* foglalkozik. Célunk, hogy felhívjuk a figyelmet a kulcscsere aktuális kérdéseire, összehasonlítva a jelenleg használt kulcscseremegoldásokat és egy új technológiát, a *kvantumkulcscserét* (*QKD – quantum key distribution*). A QKD pár éve hagyta el a laboratóriumi fejlesztés lépcsőfokát. Egyelőre bizonytalan számú, kevés adásvétel történt, és QKD-terméket alkalmazó szervezetet nem is ismerünk. A téma tanulmányozása viszont az információ értékének újragondolására késztet, miközben olyan izgalmas kérdések merülnek fel, mint hogy mennyit adnánk a tökéletes biztonságért cserébe.

A jelenleg használt hagyományos kulcscseremegoldások biztonságossága többek között egy kiszámíthatósági problémán alapul. A kicserélt kulcs kompromittálódik – és így később a felek között váltott üzenetek jogosulatlanul elolvashatóvá válnak –, ha az üzenetváltás támadója megoldja az elektronikus üzenet bizalmasságának erősségét definiáló matematikai feladatot. A mai számítógépek képtelenek az információ elévülését megelőzően megoldani ezeket a problémákat. A technológiai fejlődés és a matematikai alapkutatások viszont olyan tudományos eredményekhez vezethetnek, amelyekkel ezen feladatok gyorsan megoldhatóvá válnak, és így veszélyeztetik a kulcscsere információbiztonságát. Az eddig tárgyalt megoldásokkal ellentétben a kvantumkulcscsere fizikai törvényszerűségekből levezethetően feltörhetetlen lenne. Az új termék viszont jelenleg hátrányokkal és korlátokkal küszködik. Ezek az ellentétek ívelnek át munkánkon, amelyben a QKD-termékeket vizsgáljuk üzleti nézőpontból.

A cikk felépítése és kérdései

Jelen munka előzményeinek tekinthetők a QKD-termékekkel foglalkozó következő cikkek: Giesecke – Länger, 2011; Ghernaouti-Hélie et al., 2008; Corker et al., 2005. A mi tanulmányunk ezekhez képest újszerű abban a tekintetben, hogy a kvantumkulcscserét mint terméket az üzleti felhasználók szemszögéből is elemzi, és nem csupán technológiai vagy gyártói oldalról.

Írásunkban a szakirodalom feldolgozásával az informatikai biztonság szervezeten belüli helyzetét is tárgyaljuk. Kitérünk arra, hogy a szervezeti hierarchiában mely szakemberek foglalkoznak ezzel a kérdéssel, illetve közöttük melyek a leggyakoribb konfliktushelyzetek. Ezután áttekintjük, hogy egy elégtelen informatikai biztonságú szervezet milyen üzleti hátrányokkal kénytelen szembenézni. Majd az informatikai biztonság három tényezőjét, a szervezeti, a technológiai és a humán faktort vizsgáljuk, a munkánk szempontjából lényeges technológiai részt középpontba állítva.

Ezt követően arról írunk, hogy a kriptográfia (vagyis titkosítás) milyen szerepet tölt be az informatikai biztonságban, majd pedig arról, hogy a kulcscsere milyet a kriptográfiában. Saját szempontunk szerint csoportosítjuk a hagyományos kriptográfiát fenyegető veszélyeket, amelyeket egyben a QKD-használat motiváló tényezőinek tartunk. Ezek után említjük a kvantumkulcscserét mint a jelenlegi kulcscserék lehetséges alternatíváját.

A következő részben az ismert kvantumkulcscsere-termékek gyártóit és tulajdonságait tekintjük át. A gyártók motivációinak felismerése csökkenti a beruházást fontolgató döntéshozó információs hátrányát. A termékek esetében három külön tényezőt állapítunk meg az eddigi korlátozott elterjedés okaként, majd ezek közül a legjelentősebbre, az árra fókuszálunk. Ezzel kapcsolatban számszerűen is igazoljuk egy kvázi helyettesítő termék létezését, amely jelentős gátat szab az elterjedésnek.

Ezt követően cikkünk elsősorban a QKD célcsoportjával foglalkozik, és egy információbiztonságért felelős vezető szemléletével tekint az új találmányra. Igyekszünk objektív összehasonlítást tenni a hagyományos és a kvantumkulcscsere-termékek között mind kriptográfiai, mind üzleti szempontok figyelembevételével. Tárgyaljuk a szervezeti információnak és biztonságának értékét, és rávilágítunk arra, hogy a tökéletes biztonságot nyújtó kvantumkulcscserét milyen információk védelmezésére érdemes használni. Ebből levezetve ajánlást teszünk, hogy mely szervezetek számára jelenthet alternatívát egy QKD-termék. A szakirodalmat idézve jövőképet adunk a találmány lehetséges elterjedésének fázisaira. Végül három különböző szcenárió kifejtésével azt vizsgáljuk, hogy az alkalmazó szervezeteknek mikor lehet érdemes beruházni a kvantumkulcscsere-termékekbe.

Cikkünk célja tehát összességében az, hogy *a kvantumkulcscserére információbiztonsági termékként* tekintsen, megvizsgálja egyedi tulajdonságait, majd választ adjon arra a kérdésre, hogy *mely szervezetek számára és mikor válhat a kvantumkulcscsere szükséges információbiztonsági beruházássá.*

Információbiztonság és IT-biztonság a szervezetben

Manapság az egyes szervezetek versenyképességéhez döntő mértékben járul hozzá az információs technológiák megfelelő alkalmazása. Ugyanakkor ezek bevonása a cég mindennapjaiba veszélyforrásokat is jelent. Az információbiztonsági szakemberek feladata e kockázatok csökkentése.

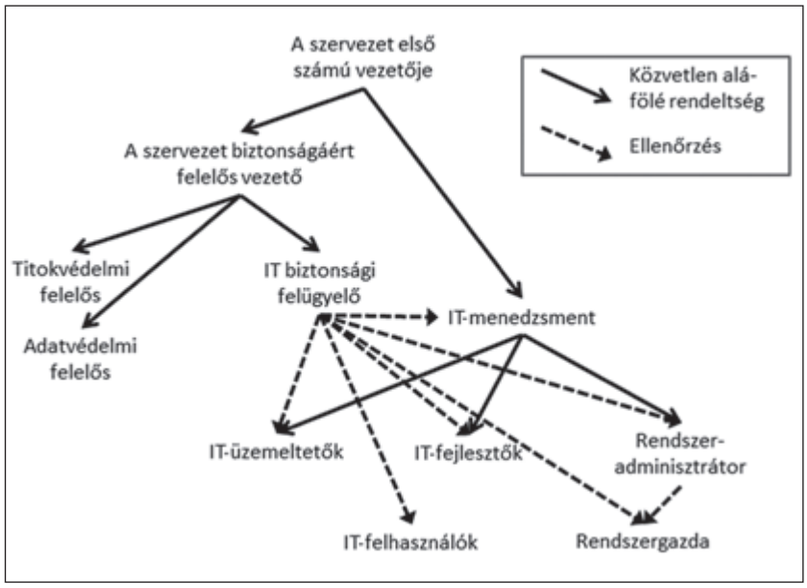
Itt hívnánk fel a figyelmet az *információbiztonság* és az *informatikai (azaz IT) biztonság* fogalma közötti különbségre. Előbbi megjelenési formától függetlenül foglalkozik az információ biztonságával, míg az utóbbi ennek csak egy részterülete: ez az ág az informatikai rendszerekben kezelt információ biztonságát állítja a középpontba. Definíció szerint az „*…informatikai biztonság a védelmi rendszer olyan, a szervezet számára kielégítő mértékű állapota, amely az informatikai rendszerekben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos*” (Szigeti et al. 2006: 5. o.).

A kellően biztonságos működéshez alapvető fontosságú az optimális szervezeti struktúra kialakítása, vala-

mint a felelősségi körök pontos meghatározása. Az IT-biztonsággal foglalkozó osztályok, személyek vállalati hierarchiában betöltött szerepe változó. Egy lehetséges elrendezést az *1. ábrán* láthatunk (Bodlaki et al. 1996: 107. o.).

1. ábra

IT-biztonsági szerepkörök



Forrás: Bodlaki et al. (1996: 107. o. alapján)

Póserné (2007) szerint az információbiztonság legfontosabb szerepköre az első számú vezetőé. Végső soron őrajta múlik a szervezeti információbiztonság megteremtésének sikeressége és minősége, hiszen az ő hatáskörébe tartozik többek között az informatikai biztonsági célok eléréséhez szükséges feltételek biztosítása. Fontos megemlíteni, hogy ez a személy gyakran nem rendelkezik informatikai ismeretekkel, a döntéseit informatikai szaktudással bíró beosztottjainak riportjai alapján hozza.

Külön kell választani ugyanakkor az információbiztonsági stratégia tervezését az operatív működéstől. Lehetséges, hogy az informatikai biztonsági felügyelő teljes döntési szabadságot kap minden kérdésben, ám a jellemző az, hogy a stratégiai kérdésekben összhang szükséges a felső vezetés, az IT-menedzsment és az egyéb, alsóbb szintű szerepkörök betöltői között. Ezt támasztja alá az is, hogy az informatikai rendszerekhez kapcsolódó befektetések szinte mindig hosszú távon kötik le a vállalat pénzeszközeit, hatásai az egész vállalatra kiterjednek – így elkerülhetetlen sokféle nézőpont figyelembevétele a döntéshozatal során.

Ez persze konfliktusokhoz vezet. Leggyakrabban az IT-menedzsment és a felső vezetés között létesülhetnek vitás szituációk, például azért, mert a két csoport eltérő szaktudásának következtében másképpen értékeli a különböző információbiztonsági kockázatokat.

Az ellentétek miatt lehet, hogy a fejlesztésre szánt pénz felhasználása kevéssé hatékony és eredményes, mennyisége elégtelennek bizonyulhat, illetve ellenkező esetben pazarló beruházásokra is sor kerülhet. Különösen érinti ez a probléma munkánk tárgyát, a kvantum kulcscserét, hiszen tipikusan egy hosszú távra szóló, drága fejlesztésről beszélünk, és mint minden biztonsági beruházásnak, ennek is nehezen becsülhető a megtérülése. Éppen ezért valódi szükségességét komoly IT-biztonsági szaktudás nélkül nem lehet megállapítani.

IT-biztonsági incidensek

Bármely beruházásnál, így az IT-biztonságban is az egyik legfontosabb feladat annak tisztázása, hogy a befektetés mely hiányosságainkra jelent megoldást. Lássuk, hogy az elégtelen információbiztonsági erőfeszítések nyomán milyen üzleti károk merülhetnek fel. Ehhez vessünk egy pillantást arra (*1. táblázat*), hogy egy adott időszakra vonatkoztatva mely ismert biztonsági incidensek okozta költségek jelenhetnek meg leginkább (Fehér, 2012).

1. táblázat

Információbiztonsági incidensek okozta költségek

Biztonsági incidens okozta veszteség	Részletezés
Üzleti hatékonyság-vesztés	▪ Kiesési idő × Érintett munkakörök bérköltsége ▪ Túlórák díja
Beavatkozási költség	▪ Szakszemélyzet időszakra vonatkozó költsége ▪ Tanácsadók, szállítók stb.
Büntetések	▪ Szabályozási okok miatt
Adatvesztés	▪ Adatok visszaállítása ▪ Hibás adatok használata ▪ Hibás döntések, késedelmes döntések
Üzleti kiesés	▪ Elmaradt bevétel (adott időszakra, kiesett szolgáltatásokból származó bevétel)
Reputációs veszteség	▪ Ügyfélszám
	▪ Ügyfélforgalom

Forrás: Fehér (2012)

A költségek becslése nem minden esetben végezhető el pontosan. Míg a túlórák díja könnyebben számolható, a reputációs veszteségből adódó ügyfélszámcsökkenésre még közelítő értéket is nehéz adni. Ez is hozzájárul ahhoz, hogy az elhárításra fordítandó összeget szintén nehéz meghatározni.

Az információbiztonság összetevői: az IT-biztonsági tréningektől a kvantumkulcscseréig

Werlinger és szerzőtársai (2008: 2–3. o.) alapján elmondhatjuk, hogy az IT-biztonság három összetevőből adódik: az *emberi*, a *technológiai* és a *szervezeti komponensekből*. Az emberi komponensek az egyén, a technológiaiak a használt informatikai rendszerek, míg a szervezetiek a különböző szervezeti egységek felelősségéről szólnak. Emberi hiba lehet a tudatlanság, technológiai hibát jelenthet egy kártékony szoftver, szervezeti szintű gondot okozhat pl. a topmenedzsment támogatásának hiánya.

Schneier (1996: 184. o.) metaforája szerint a biztonságra láncként kell tekinteni. Bármely biztonsági összetevő gyengesége miatt elszakadhat a lánc, és így az információbiztonság elveszhet. Ebből következően minden összetevő fontos, egyiket sem lehet figyelmen kívül hagyni; csupán gyengébb és erősebb láncszemeket lehet megállapítani.

Szemléltetésképpen tekintsünk a *2. ábrára*, amely a fő biztonsági összetevőket ábrázolja. A technológiai komponens alábontása – saját láncfüzére – a kriptográfia, a kriptográfiáé pedig a kulcscsere. Ebből következik, hogy amennyiben a kulcscsere nem biztonságos, úgy a kriptográfiai biztonság, magasabb szinten pedig a technológiai biztonság sérül. Egy gyenge kriptográfiai biztonságú szervezet kiváló célpontja lehet támadásoknak, ez pedig az *1. táblázatban* felsorolt negatív üzleti következmények mindegyikéhez hozzájárulhat.

2. ábra

Az IT-biztonság összetevői

Forrás: saját fejlesztés (Werlinger, 2008 alapján)

A kriptográfia és a kulcscsere helye az információbiztonságban

A *kriptográfia (avagy titkosítás)* tehát a szervezeti IT-biztonság egyik technológiai komponense. Azért felel, hogy a bizalmassági, sértetlenségi, letagadhatatlansági stb. elveket kielégítse. Mindehhez hagyományosan matematikai módszereket használ fel. Természetesen a kriptográfia is csupán láncszemként viselkedik a biztonságban. Fontos, hogy a kriptográfia szerepét ne becsüljük se alul, se felül. Érdemes tudni, hogy általában erősebb védelmi láncszemként tartjuk számon, melynél léteznek könnyebben támadhatóak.

Az ún. *kulcs* rendkívül fontos fogalom a kriptográfiában. Egy kétszereplős kommunikációban a felek akkor elégíthetik ki információbiztonsági igényeiket, és védhetik meg a közös üzeneteiket a támadóktól, ha legalább egyikük vagy pedig mindkettejük olyan ismeret birtokában van, aminek birtokában a támadók nincsenek. Ez az ismeret a *kulcs*. A kulcs ismeretében lehet az eredeti, bárki által értelmezhető *nyílt szöveget* olyan *titkosított szöveggé* alakítani (*titkosítani*, *rejtjelezni*), amelyet a támadók szándékoltan nem tudnak értelmezni; és szintén egy kulccsal lehet a titkosított szöveget nyílt szöveggé transzformálni (*visszafejteni*).

A *kulcscsere-protokollok* olyan szabályrendszerek, melyek annak levezénylésében segítenek, hogy a tényleges kommunikáció megkezdése előtt a két fél biztonságosan közös kulcshoz jusson, természetesen azt elkerülve, hogy illetéktelen szereplőhöz kerüljön a közös ismeret. Ha a támadó szert tenne a kulcsra, könnyen visszafejthetné a titkosított üzenetet, ezért a kulcscsereprotokolloknak megbízhatóaknak kell lenniük. Ezt más kriptográfiai építőelemek, ún. *primitívek* ügyes használatával lehet elérni; a legnevesebb ilyen primitív az információbiztonsági márkanévként is szolgáló *RSA*. Egy másik klasszikus példa kulcscsere-protokollra a *Diffie–Hellman-kulcscsere.*

A hagyományos kulcscsere használatának kockázatai

A jelenleg használatos kulcscsere-módszereket biztonságosnak tekintik. Ezek mind matematikai módszerek, melyekben *az információ biztonságát (többek között) egy matematikai probléma megfejtésének nehézsége garantálja*. Képletesen úgy lehet mondani, hogy a támadó képes a kulcscsere bizalmasságát kompromittálni, ha kiszámítja annak a feladatnak a megoldását, ami a kulcscsere mögött húzódik. Ehhez nincs másra szüksége, mint számítási kapacitásra, azaz számítógépre. A mostani feladatok azonban olyan komplexek, hogy nem ismerünk olyan megoldási módszert, amellyel azelőtt meg lehetne oldani őket, hogy a védeni

kívánt információ elévülne. Ez az időtáv években, évtizedekben mérhető, ami a felhasználók jelentős részének elegendőnek tűnhet.

Azt a kedvező állapotot, hogy a feltörés nehézkesnek bizonyul, a tudományos fejlődés felboríthatja. A *jelenlegi rendszerek biztonsági kockázatait* három csoportra javasoljuk elkülöníteni. Mind a három jelenség a gyorsabb vagy hatékonyabb számítás lehetőségét hordozza magában. Ezekre a tényezőkre a továbbiakban mint *a kvantumkulcscsere alkalmazásának motiváló tényezőire* hivatkozunk.

1. *A számítási kapacitás állandó növekedése.* Az informatikában trend a processzorok számítási teljesítményének fokozatos emelkedése. A számítógépek száma is folyamatosan nő, így egyre több, egyre nagyobb számítási kapacitású egységet lehet egy adott számolási feladat közös elvégzésére kijelölni. Érdemes tudni, hogy ez ellen a trendszerű növekedés ellen a használt kulcs szintén egyenletes változtatásával – ún. *hosszának növelésével* – jól meg lehet védeni aktuális bizalmas üzeneteinket.
2. *A hatékony klasszikus matematikai módszerek.* Egyetlen mostanság használatos kulcscsereeljárás esetében sincsen bebizonyítva, hogy nem lehet hatékony támadást – azaz: feladatmegoldást – kifejleszteni ellene. Ugyan a matematika nem tartja valószínűnek egy ilyen áttörés bekövetkeztét, sosem lehet kizárni az esélyét, főleg mivel egy erre irányuló kutatásnak komoly anyagi előfeltétele nincsen.
3. *A kvantum-számítógépek.* Bár ez a lehetőség igencsak a jövőbe mutat, egy dolog miatt érdemes megemlíteni. A kvantum-számítógépek önmagukban még csak laboratóriumi eredmények, de már fejlesztettek rájuk olyan programot (Shor 1995), amely képes a mai kriptográfia alapjait megingatni, és a jelenlegi kulcscsereeljárásokat használhatatlanná tenni. Így ha egy ilyen eszköz valaha is megvalósul, a kriptográfia világa minden kétséget kizárólag megváltozik.

Fontosnak tartjuk külön kiemelni, hogy *a hosszú távon értékes információk biztonságára több figyelmet kell áldozni*. Olyan támadások is elképzelhetők, amelyek a jelenlegi kommunikációnk titkosított üzeneteit csak elfogják, de feltörésükkel várnak addig, amíg ki nem fejlődik egy olyan technológia, amely képes arra. Ha feltesszük, hogy ez öt év múlva történik meg, viszont mi tíz évig szerettük volna biztonságban tudni adatainkat, akkor máris bekövetkezett a baj. Természetesen ezzel nehéz számolni: lehetetlen megjósolni, hogy az elkövetkezendő években lesz-e olyan áttörés a matematikában, amelyekkel a mostani titkosított üzeneteinket könnyűszerrel fel lehet törni. A számítási kapacitás trendszerű növekedése viszont – hiszen a jelenség bekövetkezése biztosnak vehető – véleményünk szerint állandó kockázatot jelent az olyan információkra, melyek elévülési ideje hosszú.

Milyen következményei lehetnek annak, ha a kulcscsere nem biztonságos? Ha feltesszük, hogy a támadó olyan módszer birtokában van, amellyel gyorsan meg tudja oldani a kulcscsere biztonságát őrző feladatot, akkor első lépésben megismeri a kicserélt kulcsot. Ennek ismeretében vissza tudja fejteni a felek közötti titkosított üzenetek tartalmát. Ez például nyilvános vezeték nélküli hálózat esetében fordulhat elő. Ha valaki a hálózaton belül ismerné a kulcsot, akkor pl. az ott történő netbankolásunk összes üzenetét el tudná olvasni, a jelszótól kezdve a tranzakció adataival bezáróan.

A kvantumkulcscsere (QKD) mint alternatíva

A kulcscserének új, minőségileg újat hordozó módszerét először Bennett és Brassard javasolta (Bennett – Brassard, 1984). 1992-ben megtörtént a szerzőpárosról elnevezett *BB84-protokoll* első kísérleti megvalósítása (ez mindmáig a legismertebb, leggyakrabban használt eljárás). A 2000-es évek elején az USA és az Európai Unió is nagyszabású kutatási projektet indított az új technológia vizsgálatára, ami 2002-ben kereskedelmi forgalomba is került.

A kvantumkulcscsere elméletileg feltörhetetlen – ellentétben a jelenleg használt kulcscseremegoldásokkal. Pontosabban kifejezve: a kommunikáló felek kvantumfizikai törvényszerűségek miatt szinte biztosan észrevesszik, ha a támadó jogosulatlanul lehallgatja kulcscsereüzeneteiket, ezáltal jelentős lépéselőnyhöz juthatnak. A felek ilyen esetben megszakíthatják a kommunikációt még az előtt, hogy a támadó a lehallgatott kulccsal elolvashatná titkosított üzeneteiket.

A QKD-hoz *külön kiegészítő (fotonkibocsátó- és fogadó) berendezésekre van szükség* mindkét oldalon, melyeket könnyű integrálni a már meglévő hálózatba. Csatornaként pedig optikai üvegszálat kell használni, amely számos szervezetnél már kiépített vagy kiépítése nem hordoz sok nehézséget.

A kvantumkulcscsere kielégíti a kulcscserélő eljárásokkal szemben általánosan megfogalmazott követelményeket (ilyen pl. a kulcshitelesítés, kulcsfrissesség stb.). E megállapításunkat egy korábbi munkánkban fejtettük ki, melyre most terjedelmi okokból csak hivatkozunk (Fülöp – Virág, 2011: 52–53. o.). Összességében elmondható, hogy *a QKD technológiailag képes azt a kriptográfiai szerepet is betölteni, amelyet ma a hagyományos kulcscsereeljárások betöltenek*, sőt sok szempontból túlszárnyalja azt.

A fentiekben kifejtettek dacára a kvantumkulcscsere az elméleti feltörhetetlenség ellenére viszont egyelőre implementációs nehézségekkel küszködik. Az érzékeny kvantumfizikai alkotórészek sebezhetőségeket jelentenek – ezek viszont más jellegűek, és csak egy technológiailag jóval felkészültebb támadó által kihasználhatóak, mint a hagyományos kulcscsere esetében.

Egy másik implementációs problémát jelent az, hogy *jelenleg tetszőlegesen hosszú csatorna nem építhető ki*. Ennek oka kvantumfizikai okokban keresendő. Azért, hogy egymástól tetszőlegesen távol lévő pontok között is megvalósulhasson a kvantumkulcscsere, különböző kutatások egyrészt a csatornahossz-növeléssel, másrészt hálózatok kiépítésével foglalkoznak.

Láthatjuk tehát, hogy a QKD-nak még vannak bizonyos hiányosságai, de a kutatók és a gyártók nagy erőfeszítéseket tesznek ezek kiküszöbölésére.

A kvantumkulcscsere-termékeknek és gyártóinak áttekintése

A kvantumkulcscsere-termékek gyártói

Néhány gondolat erejéig érdemes a kínálati oldal szereplőire is tekinteni, hiszen ha kvantumkulcscsere-beruházást tervezünk, onnan fog kikerülni leendő partnerünk. Világszerte összesen három vállalat árusít kvantumkulcscsere-termékeket: egy az Egyesült Államokban, egy Svájcban és egy Ausztráliában. Hogy miért lehet ilyen alacsony e vállalatok száma, arra a fejezet későbbi szakaszaiban világítunk rá.

Az *amerikai MagiQ* szoros összefüggésben áll az Államok védelmi minisztériumával, és kereskedelmi partnerei között a NASA-t is megtaláljuk (MagiQ, 2012a).

A *svájci ID Quantique* volt az első vállalkozás, mely 2002-ben kereskedelmi forgalomban elérhetővé tette termékeit (Quantum Information Partners é. n.: 1. o.). A Genfi Egyetem spin-off cégének három üzletága van (ID Quantique, 2011a): (1) hálózattitkosítási üzletág, mely a QKD-termékeken túl számos hagyományos titkosító berendezést is gyárt, (2) alkatrészgyártói – pl. fotonkibocsátók, fotondetektorok – üzletág, illetve (3) kvantumfizikán alapuló véletlenszám-generátort gyártó üzletág. A vállalat a számos partnercégből ítélve – joggal – legalább egész Európát tekinti piacának. Hazánkban is rendelkezik partnerrel, könnyebb lehetőséget teremtve a kvantumkulcscsere-termékekben gondolkodó hazai szervezetek számára.

Az *ausztrál Quintessence Labs* az Ausztrál Nemzeti Egyetem spin-off cége. A társaság weboldalán nem találtunk konkrét információt a termékkínálatról, csupán szakmai eredményeikről szóló beszámolókat (Quintessence Labs, 2012).

Véleményünk szerint a helyettesítő termékek jelentős fenyegető ereje miatt e vállalatok pillanatnyilag nem egymás ellen versenyeznek, sokkal *több erőforrást fektethetnek a potenciális vásárlók meggyőzésébe*. Érdemes tudni, hogy a piacon az első publikus adásvételek az elmúlt 1-2 éven belül történtek – jóllehet a vevők személye nem ismert.

Mindhárom cég viszonylag kevéssé ismert kis- vagy középvállalkozásnak mondható. Ez az ismeretlenség a lentebb bővebben kifejtett bizalomhiány mint terjedésgátló tényező megszűnésének nem kedvez, illetve az egyes szakértők által kulcsfontosságúnak tartott tömegtermelés beindítása sem várható tőlük.

De nagy technológiai vállalatok is foglalkoznak már ezzel a témával. A Siemens a jövőben teljes körű, kvantum kulcscserén alapuló szolgáltatáscsomagokat kíván a fogyasztók felé nyújtani, melyeknek a hardver, a szoftver és az infrastruktúra egyaránt része. Nem lát fantáziát viszont QKD-berendezések gyártásában. Ezzel összhangban 2009 augusztusában megállapodás született a Siemens és az ID Quantique között (Graham – Rove, 2009).

Más nagyvállalatok is folytatnak kutatásokat a kvantumkriptográfia témakörében, a teljesség igénye nélkül ezek a következők: Fujitsu, HP, IBM, Mitsubishi, NEC (Quantum Information Partners, é. n.: 1–6. o.). Véleményünk szerint a kvantumkulcscsere tömeges elterjedése ezektől a vállalatoktól várható, vagy saját termék kiadása, vagy a fentebb bemutatott vállalatokkal való együttműködés, felvásárlás következtében.

Ezt azzal indokoljuk, hogy az új termékkel szembeni bizalom megnövelésére az ismert informatikai piaci márkanevekkel való szoros stratégiai kapcsolat fenntartása szükséges. Illetve, ahogy Corker és szerzőtársai (2005) is megfogalmazzák, a közös meggyőzési probléma leküzdésére a gyártó cégek közötti társulás javasolt, amely pl. a szakmai események marketingerejét használhatná fel.

Javasoljuk a hagyományos kulcscsere fentebb ismertetett kockázatainak – legalábbis az IT-n belüli – köztudatba ültetését, valamint a QKD-termékek ismert szabványoknak való megfeleltetésének sürgetését.

A fentiekből következően valószínűsíthető, hogy egy potenciális vásárló vállalat képviselője szakmai konferenciákon hall először QKD-termékekről, feltehetően feltörhetetlen csúcstechnológiaként. Álláspontunk szerint arra is fel lehet készülni, hogy a forgalmazó tudatosan kihasználja a vevői alulinformáltságot. A beruházás megfontolása során tehát figyelmet kell fordítani a valós információbiztonsági és üzleti szempontokra. Erről szólunk még tanulmányunkban.

A gyártóknak külön nehézséget okozhat, hogy *egyes országokban a mai napig korlátozzák a kriptográfiai termékek importját-exportját*, de jellemzően ezek a korlátozások csökkennek, illetve az EU-n belül nem léteznek. Importjuk az EU-n belül teljesen szabad, EU-n kívüli országból ún. nemzetközi importigazolás megléte szükséges hozzá. Egyébiránt Magyarországon a 2004. évi 50. kormányrendelet kimondja, hogy titkosítási termék exportálása engedélyezett.

A kvantumkulcscsere-termékek jellemzése és elterjedésük korlátozó tényezői

Az implementációs nehézségeket leküzdve, vagy ezek ellenére elérhetőek már kulcsrakész kvantumkulcscsere-termékek. Tudomásunk szerint az említett három vállalat közül csak kettő árusít ilyen fejlettségű termékeket.

Az *ID Quantique* honlapja (ID Quantique, 2011a) szerint jelenleg egy QKD-berendezéssel, a *Cerberis*szel vannak jelen a piacon. A termékspecifikáció (ID Quantique, 2010) 100 km-re szabja meg a két kulcscserélő szerver maximális távolságát, mely szervereket szabványos optikai kábel köti össze. Az eszköz a legkorszerűbb kvantumkulcscsere-protokollokat és titkosítási eljárásokat használja. Kompatibilis a széles körben elterjedt, ún. Ethernet hálózatokkal.

A vállalat a honlapján szűkszavúan ismerteti a Cerberishez köthető eddigi „számos" adásvételét – ezek egyfajta anonim referenciaként szolgálnak –, és csupán kettőt emel ki közülük.

A terméket először 2007-ben Genfben egy *helyi elektronikus szavazáson használták* (Messmer, 2007; Dodson et al., 2009: 17–18. o.). A kvantumkulcscsere két végpontja közül az egyik egy szavazatszámláló központ volt, ahová az összes papír- és elektronikus alapú szavazat befutott és megszámláltatott, a másik pedig a genfi kanton adattárolója, ahol a választási adatokat archiválták. Ezek után a sikeres kulcscserével kicserélt kulccsal rejtjelezett választási adatok egy szokásos hálózati összeköttetésen folytak át.

Másrészt egy, a pénzügyi szektorban jelenlévő, meg nem nevezett vállalat is a Cerberis kulcscsereszerver bevezetése mellett döntött (ID Quantique. 2011b). A kvantumkulcscsere a cég központja és egy attól mintegy 50 km-es távolságban lévő adat-helyreállító központ között történik. A cég honlapján található esettanulmány kiemeli annak fontosságát, hogy az eszköz kezelése és monitorozása grafikus felhasználói felületen, távolról, biztonságosan is megtörténhet.

A másik kulcsrakész eszközt kínáló cég a *MagiQ*. A vállalat weboldalán a *QPN-8505*, valamint a *Q-Box Workbench* nevű berendezéseket láthatjuk forgalmazott termékként. A QPN-8505 specifikációját tekintve meglehetősen hasonlít a Cerberisre: QKD-protokollja, titkosítási primitíve, hatótávolsága egyezik a svájci cég termékével (MagiQ, 2007). A Q-Boxot a kvantumkulcscsere alkalmazásának kutatására lehet hasznosítani; elsősorban egyetemek, kormányzatok és óriáscégek tudósai számára ajánlják (MagiQ, 2012b).

A mindössze néhány gyártó cég és a bizonytalan, a hagyományos kulcscseretermékekhez képest feltehetően elhanyagolható mennyiségű adásvétel miatt azt gondoljuk, hogy a kvantumkulcscserébe való befektetés – alkalmazói oldalról – napjainkban még kevéssé vonzó, még akkor is, ha a kvantumkulcscserét a hosszú távon is értékkel bíró információk védelmének esetében kriptográfiailag szükségesnek ítéljük.

Álláspontunk szerint jelenleg *három fő oka* lehet annak, hogy a kvantumkulcscsere nehezen terjed el. Egyrészt a túlságosan *magas ár* elriasztja a vevőket, hiszen létezik egy kvázi helyettesítő termék, a hagyományos kulcscsere, mely töredékáron elérhető. Másrészt a jelenlegi *technológiai problémák és korlátok* sem teszik vonzóvá a megoldást. Harmadrészt pedig, mint minden merőben új terméket, ezt is *bizalmatlansággal* fogadja először a keresleti oldal. Az első említett tényezőt vizsgáljuk meg alaposabban a következőkben.

A kvantumkulcscsere-termékek árának kérdése a hagyományos megoldások tükrében

Az ID Quantique Cerberis termékének ára kb. *100.000 dollár* (Quantum Information Partners é. n.: 1. o.), míg a MagiQ-féle QPN-8505 áráról nincs információnk, de az elődjének tekinthető QPN-7505 *98.000 dollárba* került (Gyöngyösi, é. n.: 64. o.).

A szakemberek különbözőképpen ítélik meg ezt a költséget. Egyikük hangsúlyozza, hogy ez a költség még *beleférhet a nagyvállalatok forintmilliárdos IT-biztonsági büdzséjébe*, melyet egyébként a teljes IT-költségvetés 10-20%-ára tett (Fekete–Szűcs, 2011). Ezzel eltérő véleményen van egy magyarországi információbiztonsági cég szakértője, aki ezt az árat *ellehetetlenítő tényező*nek tartotta (Balázs, 2010). Az ő szavait erősíti Christian Monyk, egy világszerte elismert kvantumkriptográfus szakember, aki 10.000 euró alá szorítaná az árat (Müller, 2009: 51. o.). Szintén az elterjedés korlátjának tartja az árat egy magyarországi kereskedelmi bank név nélkül nyilatkozó szakértője, aki csak *a hagyományos eljárásoknál 2-3-szor magasabb összeget tartana elfogadhatónak* – vagyis csak mint tömegtermék tartja reális alternatívának a QKD-t (F–B, 2011).

Mi nem szeretnénk egyik oldal mellett sem állást foglalni. Ennek egyik oka az, hogy a termékek árai szerintünk vevőről vevőre változóak, mert személyre

szabást igényelhetnek – például a csatlakoztatni kívánt számítógépek száma lehet ármódosító tényező. Másrészt azzal sem vagyunk tisztában, hogy a meghirdetett árak mit takarnak: csupán a hardverelemeket, vagy tartalmazzák a bevezetés költségét, esetleg valamennyi időre szóló terméktámogatást is?

A *hagyományos titkosítási eljárások díja* viszont mindenképpen más nagyságrendű. A költség szinte kizárólag az ún. *nyilvános kulcstanúsítvány megszerzésének díjából áll* (F–B, 2011). A tanúsítvány egy megbízható szervezet – ún. *hitelesítésszolgáltató* (CA) – által kibocsátott igazolás, amely a használt kriptográfiai kulcsok hitelességét bizonyítja.

Az egyik legnevesebb hitelesítésszolgáltató, a VeriSign legnagyobb hitelességet adó tanúsítványa 1.499 dollárba kerül egy évre, adók nélkül (VeriSign, 2011). Azonban a kereskedelmi bank szakértője elmondta, hogy belső használatra, tehát például két telephely között nem is CA általi, hanem saját kiadású, ingyenes tanúsítványokat használnak (F–B, 2011).

Elmondhatjuk tehát, hogy *a kvantumkulcscserének jelenleg egy szinte elhanyagolható költségű, közeli helyettesítő terméke van*, a hagyományos kulcscsere. Mi ezt tartjuk az elterjedést gátló tényezők közül a legfontosabbnak, és ezzel magyarázzuk a forgalmazó vállalatok rendkívül alacsony számát.

Döntés kvantumkulcscsere-termék bevezetéséről

Az előzőekben már említettük, hogy az IT-menedzsment és a felső vezetés közötti vitás szituációk legfőbb oka az eltérő szaktudás. A kvantumkulcscsere radikálisan újszerű volta következtében azonban lehetséges, hogy az IT-menedzsment sem elég informált a kérdésben. Ezért mindenképpen javasoljuk a témát a vállalati hierarchiában esetleg alacsonyabb szinten lévő kriptográfiai szakemberrel megvitatni.

Ez a fejezet egy ilyen megbeszéléshez nyújt támpontokat. A megalapozott döntéshez szükséges a hagyományos és az új megoldás információbiztonsági és üzleti szemléletű összehasonlítása, a védendő információ értékének megbecslése, a piac kvantumkulcscserével szembeni viselkedésének megértése, illetve az új technológiával kapcsolatos döntés előnyeinek és hátrányainak pontos ismerete. Tárgyalásunk utolsó fejezetében ezekkel foglalkozunk.

A hagyományos és kvantumkulcscsere-termékek alkalmazásának összehasonlítása

Jelen pontban minél több szempont bevonásával összevetjük, hogy egy információbiztonságért felelős döntéshozó számára milyen érvek szólnak a kvantumkulcscsere-termékek használata mellett illetve ellen. Elemzésünkben mind az kriptográfiai, mind az üzleti aspektust figyelembe vesszük.

Nem kérdéses, hogy az új technológia alkalmazása a kereslet oldaláról jelentős beruházást igényel. Ha megvalósul, azt alapos költség-haszon elemzésekkel fogják indokolni, melyből kiolvasható, hogy a beruházást érdemes megvalósítani.

Tekintsük először, némileg leegyszerűsítve, a *kriptográfiai nézőpontot*! Ehhez elsősorban a hagyományos matematikai kulcscsere-eljárások használatának már ismertetett kockázataira kell tekintettel lenni. Minthogy ezen eljárások feltörésének rendkívül alacsony – igaz, teljesen ki nem zárható – esélye van, használatuk általában véve biztonságosnak tekinthető. Ugyanakkor egy népszerű meglátás szerint a kockázat mértékét nemcsak a *veszély bekövetkezésének valószínűsége*, hanem az általa *esetlegesen okozott kár nagysága* is befolyásolja. Ha döntéshozónk igazán körültekintő, megpróbálkozhat ezzel a nehéz számszerűsítési feladattal – az információ értékének megragadásával később bővebben foglalkozunk.

Véleményünk szerint mindehhez tekintetbe kell venni a *védelmezni kívánt információ elévülési idejét* is, hiszen, mint kifejtettük, a hosszú távon is értékes (bizalmas) információk nagyobb veszélynek vannak kitéve. Mivel a kvantumkulcscsere egy bizonyítottan feltörhetetlen kulcscsereeljárás, ha egyéb kriptográfiai eszközeinkben megbízunk, a kvantumkulcscsere használatával *már a jelenben örökké szóló kriptográfiai védelmet lehet nyújtani a kulcscserének, és így az arra épülő bizalmas elektronikus kommunikációnak*. A titkosított üzenetek feltörési kísérleteinek sikerességeivel folyamatosan tisztában kell lenni. *Egy olyan jövőben, amelyben a hatékony feltörések miatt nem támaszkodhatunk a hagyományos kulcscserére, a kvantumkulcscsere nélkülözhetetlen lehet egy tökéletesen biztonságos elektronikus kommunikáció lebonyolításához.*

A döntéshozáshoz ismerni kell a QKD jelenlegi implementációs problémáit is. A használt kvantumfizikai berendezések esetleges pontatlanságát, érzékenységét kihasználva észrevétlenül le lehet hallgatni a kulcscserét, ezáltal kompromittálva a kulcs bizalmasságát. A különböző támadási módszerek áttekintéséhez korábbi munkánkat javasoljuk (Fülöp – Virág 2011: 33–36. o.). Összességében kijelenthető, hogy e támadások kivitelezéséhez a támadónak is a feladatnak megfelelő, magas szakértelmet és tőkét igénylő eszközök szükségesek. Véleményünk szerint tehát nem szabad elsiklani a létező hiányosságok felett, de a fentiek miatt a lehetséges támadók köre QKD-technológiára váltva mindenképpen szűkül.

A legfontosabb *üzleti szempont* az új termék bevezetésének tervezésénél természetesen a már említetten igen magas ár. Mint fentebb kifejtettük, a hagyományos kriptográfia használatának költsége jóval kisebb, és sok esetben elhanyagolható, míg a QKD-termékek ára a 100.000 dolláros (azaz 20 M Ft-os) nagyságrendben helyezkedik el.

A hagyományos titkosításokhoz képest ez feltétlenül drága, ugyanakkor számításba kell venni a következőket is: egyrészt csekély infrastruktúraigénye miatt *bevezetésekor alig szenved csorbát az üzletmenet-folytonosság*, másrészt a QKD végső megoldást jelent, és *elméletileg nem igényel további, kriptográfiai igényekből keletkező fejlesztéseket* (Ghernaouti-Hélie et al., 2008: 15–16. o.), ellentétben a támadások erősödésével folyamatosan változtatandó hagyományos kulcscsereeljárásokkal.

Mindemellett, ha egy szervezet csúcstechnológiát használ, önmagában is előnyös, ha ezt érintettjei tudomására hozza: egy ilyen szervezet felé *megnő a bizalom*. Nemcsak azért, mert azok pl. nagyobb biztonságban érzik adataikat, hanem mert tudják, hogy a vállalat nyitott a fejlődésre, jobb technológiát használ, mint a versenytárs, és hogy nem mellesleg a szervezet anyagilag jól áll. Ezek az érvek persze javarészt az információs aszimmetrián alapulnak. Az érintettek túlnyomó többsége nem ismeri a kriptográfiai hátteret, nem gondol bele, hogy a kevés tapasztalat a QKD-termékekkel kapcsolatban milyen veszélyeket rejt, és lehet, hogy nem foglalkozik azzal, hogy a beruházás költsége a cég termékeinek árán is érződhet a későbbiekben.

Nem szabad megfeledkezni a különféle *szabályozásoknak való megfelelésről* sem. Például a 2002 óta minden amerikai tőzsdén részt vevő vállalat számára kötelező Sarbanes–Oxley-törvény úgy fogalmaz, hogy „*a lehető legteljesebb mértékben védeni kell az információvagyont*". A Bázel II szabályozáscsomag működésikockázat-szemlélete, illetve az Európai Unió elektronikus hírközlési adatvédelmi direktívája szintén információbizalmassági feltételek teljesülését követeli. A QKD segítségével ezek a követelmények minden eddiginél jobban betarthatóak (Ghernaouti-Hélie et al., 2008: 13. o.). Ha a jövőbe tekintünk, a kockázatalapú szemlélet a 2010-es évek végére fokozatosan érvénybe lépő Bázel III szabályozásokban is él, magukba foglalva a pénzügyi szervezetek felé támasztott információbiztonsági igényeket is.

Végül tegyünk említést az üzleti szempontból vett bizonytalanságokról is. A bevezetésnél mindenképpen bizonytalanságot okoz a kvantumkulcscsere használati *referenciák hiánya*. Mint említettük, nyilvános információ nem létezik arról, hogy valamely kereskedelmi szervezet napi működésében használná az új találmányt; ebből kifolyólag még a használati tapasztalatok is hiányoznak. A bizonytalanság okozta negatív tényezőt némileg ellensúlyozza a csúcstechnológia alkalmazásának fentebb kifejtett pozitív hatása.

A kvantumkulcscserének egy információbiztonsági rendszer kisebb, de fontos részeként mindenképpen illeszkednie kell a már meglévő és a jövőbeli hardverkörnyezetbe és infrastruktúramenedzsment-eljárásokba. Az illeszkedést igazolhatják a *szabványoknak való megfelelésről szóló tanúsítványok* – az IT-biztonság területén ilyen szabvány pl. a Common Criteria feltételrendszere, de arról nincsen információnk, hogy a jelenlegi termékek ennek megfelelnének. Még nem létezik olyan szabvány, amely specifikusan a QKD-technológia megfeleléséről szólna, ugyanakkor ezen az ETSI (Európai Híradástechnikai Szabványügyi Intézet) ISG-QKD nevű munkacsoportja 2008 óta dolgozik (l. Giesecke – Länger, 2010). A beruházásról döntést hozónak biztosan érdemes követnie e szabványosítási procedúrát.

Az információnak és biztonságának értéke, célcsoport és elterjedés

Ebben a szakaszban azzal foglalkozunk, hogy mennyi pénzt érdemes információbiztonságra költeni. Írásunk kapcsán a kérdés azért releváns, mert a kvantumkulcscsere komoly beruházást igényel, és lehetséges, hogy a védendő információ értéke ezt nem indokolja.

Az információ értéke egyenlő a hasznosságának és beszerzési költségének különbségével. Így egy információ értéke attól függően változik, hogy kinek a birtokában van. De mennyit érdemes információbiztonságra költeni? Széles körben elterjedt vélemény, hogy maximum annyit, amennyit ér nekünk. Ezért elméletileg a biztonságra fordítandó összeg felírható a következő formában:

$$C \leq P_1 \times V_1 + P_2 \times V_2 + \ldots + P_n \times V_n,$$

ahol P_x egy lehetséges x támadás bekövetkezésének valószínűsége, V_x pedig az x támadás által okozott kár. Az összeadás tagjai az *1. táblázatban* látható biztonsági incidensekre vonatkozhatnak. A számolást nehezíti, hogy a $P_1,\ldots, P_n$ és a $V_1,\ldots,V_n$ értékeket csak becsülni lehet, és hogy nem kell minden támadástípushoz más védelem, ezért az összeadás tagjainak számát, és így C-t csökkenteni lehet valamennyivel. Arról sem szabad megfeledkezni, hogy egy bizonyos támadás bekövetkeztének valószínűsége végtelen időhorizonton 1, azaz a költségbecslést bizonyos időtartamokra kell elvégezni.

Az általunk megkérdezett információbiztonsági szakemberek közül az egyikük úgy fogalmazott, hogy ezt az összeget úgy lehet mérni, hogy *meghatározzuk azt az összeget, amit a kármentésre szánnánk abban az esetben, ha a fejlesztésre nem kerülne sor* (Fekete–Szűcs, 2011). Ez egy más megfogalmazása az általunk fentebb leírt képletnek.

Egy kereskedelmi bank információbiztonsági vezetője viszont kifejtette, hogy „*…annyit kell költeni, amennyi a »beidézhető« veszteség és a reputációs veszteség összege*". Tehát a stratégiai fontosságnál esetenként többet (F–B, 2011). A bank egy másik szakértője ehhez még hozzátette, hogy egy esetleges adatlopás minden következményével számolni kell, amikor a védelemre fordított pénzt kalkuláljuk, például a jogi vonatkozásokkal is.

Mely szervezeteknek éri tehát meg a kvantumkulcscsere alkalmazása? Azoknak, melyeknél egy esetleges támadás által okozott kár magas, illetve ez nagy valószínűséggel következik be. Ezek meglátásunk szerint

- *olyan szervezetek, melyek az információt stratégiai fontossága miatt védik*: például egy gyógyszergyár, amelynek kutatásai eredményeinek bizalmassága elsődleges, vagy
- olyan szervezetek, *melyeknek komoly kötelezettségük áll fenn érintettjeik személyes adatainak védelmére*, és az adatbizalmasság sérülése esetén az érintettek közvetlenül, a szervezet pedig közvetetten szenvedne hátrányt: erre példaként ügyféladatokkal dolgozó bankok, állami szervezetek említhetők.

A szakirodalom szerint a kvantumkulcscsere elterjedése hasonlatos lehet a hagyományos titkosítások elterjedéséhez. Ez látható a *3. ábrán*.

Azt, hogy ezek a fázisok pontosan mikor fognak megtörténni, nehéz megjósolni, hiszen a motiváló tényezők bekövetkezéséhez sem rendelhető pontos időpont. A Gartner informatikai tanácsadó cég 2011-es, a feltörekvő technológiákat vizsgáló ún. *hype görbéje* szerint a kvantum-számítógépek elterjedése csak több mint tíz év múlva várható (Gartner, 2011). Ugyanakkor egy matematikai áttörés akár már holnap bekövetkezhet.

A bevezetés időpontjának kérdése

Az előző szakaszban a kvantumkulcscsere globális elterjedéséről beszéltünk, de nem árt megvizsgálni azt sem, hogy egy adott szervezetnek mikor, milyen feltételek mellett érdemes hozzájutni az új technológiához. Saját elemzésünkben három választási lehetőséget fejtünk ki. Azt nézzük, mi történik, ha

- (1) manapság,
- (2) néhány év múlva, de még egy motiváló tényező bekövetkezése előtt, vagy
- (3) egy motiváló tényező bekövetkezése után

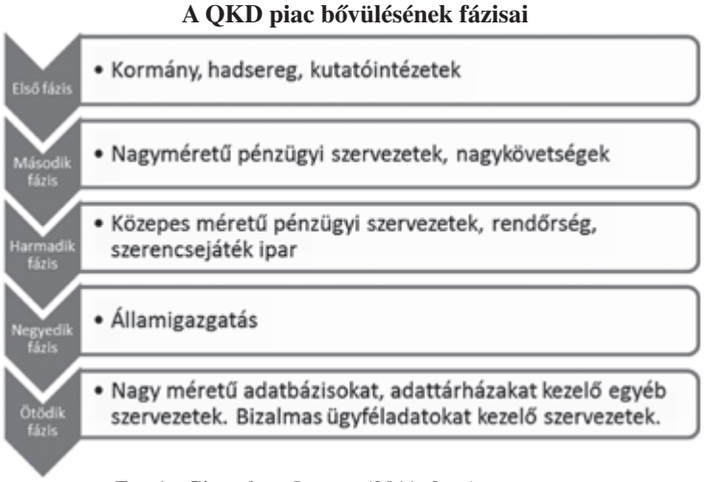
vesz egy cég kvantumkulcscsere-terméket.

(1) Ha mostanában ruház be egy cég az új technológiába, azt pusztán kriptográfiai okokkal nehéz indokolni. Hiszen jelenleg csak az örökké szóló kriptográfiai védelmet kívánó bizalmas elektronikus kommunikációnak van szüksége az új technológiára, a többi kommunikáció napjainkban biztonságosnak mondható. Persze az azonnali beruházással egy váratlan matematikai áttörést követő versenyelőny gyorsan jelentkezne. De egy mostani beruházás esetén a legvalószínűbb egy technikai probléma felmerülése, illetve egy sikeres támadás kivitelezése. A magas ár, a szűk kínálat, a szabványok hiánya és a csekély számú referencia szintén hátrányos. A pénz időértékét tekintve is ez a legrosszabb megoldás. Ugyanakkor cégünk innováció felé való nyitottságát is kifejezhetjük a vásárlással.

(2) A második esetben azt az állapotot vizsgáljuk, amikor még nem történt matematikai áttörés, a számítási kapacitás növekedésével a hagyományos kriptográfia kulcshosszai egyre növekednek, és a kvantum-számítógépek fejlettségi foka is egyre inkább fenyegeti az eddigi eljárásokat. Nehéz megbecsülni, hogy mikor számíthatunk erre az állapotra. A kriptográfiai indoklás nehézsége az előző esethez mérhető. Mivel jelenleg több óriásvállalat is folytat kutatásokat írásunk témájában, úgy gondoljuk, hogy ekkorra már kínálatbővüléssel kell számolni. Ez az árat lefelé nyomja, a referenciák hiányának problémája már kevésbé égető. A nagy cégek piacra lépésével a szabványosítás is könnyebbé válik. A termék viszont veszít az innovatív értékéből.

3. ábra

A QKD piac bővülésének fázisai



Forrás: Giesecke – Länger (2011: 3. o.)

(3) A harmadik esetet kettébontjuk aszerint, hogy a motiváló tényező mikor és hogyan következik be. A kriptográfiai szükségesség mindkét eshetőség bekövetkezésekor egyértelmű. Az első eset az, hogy a közeljövőben váratlanul kerül sor egy matematikai áttörésre, ami a jelenlegi kulcscsere-metódusok biztonságát megszünteti. Ekkor a kereslet óriásira duzzad, amit a jelenlegi három kis cég nem tud kielégíteni. A támadók lépéselőnybe kerülnek, a termékek ára az egekbe szökik, a kvantumkulcscserét már idejében beszerző cégek jelentős versenyelőnyre tesznek szert. A másik eset például akkor játszódik le, amikor a kvantum-számítógépek képesek lesznek feltörni a hagyományos kulcscseréket, de az eseményre a gyártók és a felhasználók felkészülnek. Ekkorra a gyártók számának növekedésével, a tömegtermelés beindulásával az árak csökkennek, a referenciákkal és a szabványokkal kapcsolatos kérdés megszűnik, de a termék innovatív jellegével már nem számolhatunk.

Összegzés

Cikkünk a vállalati információbiztonság témáján belül áttekintést ad egy, a laboratóriumi fejlesztés fázisát nemrég elhagyó, minőségileg új termék, a *kvantumkulcscsere* (*QKD*) bevezetésének műszaki és üzleti vonatkozásairól.

Csoportosítottuk az ezt a funkciót klasszikusan betöltő hagyományos kulcscsereeljárások használatának kockázatait, amelyek véleményünk szerint egyúttal a QKD használatának motiváló tényezői is. Ebből kiindulva állapítottuk meg az új találmány szükségességét: a jövőben elkerülhetetlen lehet a használata, de a hosszú távon értékes, bizalmasságot igénylő információk védelme érdekében akár már most is az.

A kvantumkulcscsere-termékek használata azonban egyelőre ritkaságszámba megy. Ennek három okát különítettük el: a túlzottan magas ár és a szinte ingyenes kvázi helyettesítő termék, a technológiai problémák, valamint az újdonsággal szembeni bizalmatlanság okozta terjedési korlátot.

Míg a gyártó vállalatoknak elsősorban a fenti három tényezővel kell megküzdeniük, a potenciális felhasználó szervezeteknek azt kell végiggondolniuk, szükséges-e számukra a kvantumkulcscsere a vállalati információbiztonságukban. Informatikai és üzleti szempontú elemzésünk összehasonlította a hagyományos és a kvantumkulcscsere-termékeket. A védendő információ értékének megbecslését a döntéshozás fontos lépésének tartjuk, és ehhez javaslatokat is megfogalmaztunk. Ebből levezetve megállapítottuk, hogy egyrészt olyan szervezeteknek érdemes a QKD bevezetését fontolóra venni, ahol az információt stratégiai értéke miatt, illetve ahol erős adatvédelmi kötelezettség teljesítése végett védik. Megvizsgáltuk a kvantumkulcscsere-technológiára való áttérés időpontjának dilemmáját három lehetséges forgatókönyv megfogalmazásával.

Úgy gondoljuk, hogy cikkünk olvasása után egy olyan megbeszélésen, melyen a felső vezetés, az IT-menedzsment és a kriptográfiai szakemberek egyaránt jelen vannak, átgondolt döntés születhet arról, hogy a szervezetben szükség van-e a kvantumkulcscsere-beruházásra, és ha igen, mikor.

Felhasznált irodalom

Bennett, C. H. – Brassard, G. (1984): Cryptography: Public key distribution and coin tossing. in: Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, pp. 175–179. Elérhető: http://www.cs.ucsb.edu/~chong/290N-W06/BB84.pdf. Letöltve: 2012. augusztus 2.

Balázs I. (2010): Kriptográfia, információbiztonság (interjú). A HunGuard Kft. telephelye, Budapest. Készítette: Fülöp Árpád, Túri Éva, Virág Péter

Bodlaki Á. et al. (1996): Miniszterelnöki Hivatal Informatikai Koordinációs Iroda Informatikai Tárcaközi Bizottság ajánlásai: Informatikai rendszerek biztonsági követelményei, 12. sz. ajánlás. Elérhető: http://www.ekk.gov.hu/hu/kib/archivum/itb/ITB12.pdf. Letöltve: 2012. augusztus 3.

Corker, D. et al. (2005): Commercial prospects of Quantum Information Processing. Elérhető: http://www.materials.ox.ac.uk/uploads/file/QIPIRC/Commercial%20Prospects%20for%20QIP%20v1.pdf. Letöltve: 2011. okt. 27.

Dodson, D. et al. (2009): Updating Quantum Cryptography Report ver. 1. Elérhető: http://arxiv.org/pdf/0905.4325v1.pdf. Letöltve: 2012. augusztus 2.

Fehér P. (2012): IT-projektek megtérülése (előadás). Elérhető: http://www.slideshare.net/pethich/it-projektek-megtrlse. Letöltve: 2012. augusztus 2.

Fekete-Szűcs L. (2011): Az információ értéke, biztonsága, stratégiai javaslatok kvantumkulcscserével foglalkozó vállalatoknak (interjú). Budapesti Corvinus Egyetem, Budapest. Készítette: Fülöp Árpád, Virág Péter

F. GY. – B. R. (2011): Információbiztonság egy bank életében (interjú). Egy nemzetközi kereskedelmi bank magyarországi központja, Budapest. Készítette: Fülöp Árpád, Virág Péter. 2011. október 25.

Fülöp Á. – Virág P. (2011): A kvantumkulcscsere jövőjének vizsgálata gazdasági szemszögből (szakdolgozat). Bp.: Budapesti Corvinus E., Információrendszerek Tanszék

Gartner (2011): Hype Cycle for Emerging Technologies, 2011 (grafika). Elérhető: http://www.gartner.com/hc/images/215650_0001.gif. Letöltve: 2012. augusztus 3.

Ghernaouti-Hélie, S. et al. (2008): SECOQC Business White Paper. Elérhető: http://www. secoqc.net/downloads/ SECOQC_Business_Whitepaper_01b.pdf. Letöltve: 2011. október 22.

Giesecke, S. – Länger, T. (2010): Promoters and Inhibitors of QKD – The Prospects of QKD – ETSI ISG-QKD (ETSI kutatási jelentés)

Giesecke, S. – Länger, T. (2011): Prospects of Quantum Key Distribution: Making Data Communication Secure for the Future. Elérhető: http://www.foresight-platform.eu/ wp-content/uploads/2011/07/EFP-Brief-No-183_QKD. pdf. Letöltve: 2011. október 27.

Graham-Rove, D. (2009): Quantum Cryptography for the Masses. Technology Review (internetes újság). Elérhető: http://www.technologyreview.com/computing/23317/. Letöltve: 2011. október 30.

Gyöngyösi L. (év nélkül): Kvantumkriptográfia I. (előadás-fóliák). Elérhető: http://www.mcl.hu/quantum/foliak/ kvantumkript1.pdf. Letöltve: 2011. szeptember 26.

Id Quantique (2010): Cerberis v3.0 – Specifications (termékspecifikáció). Elérhető: http://www.idquantique. com/images/stories/PDF/cerberis-encryptor/cerberis-specs.pdf. Letöltve: 2011. október 13.

Id Quantique (2011a): ID Quantique SA – Network Encryption, Random Number Generators, Photon Counting (weboldal). Elérhető: http://www.idquantique. com/. Letöltve: 2011. október 27.

Id Quantique (2011b): 10G Ethernet Encryption for Disaster Recovery Center. Elérhető: http://www.idquantique. com/images/stories/PDF/cerberis-encryptor/user-case-drc.pdf. Letöltve: 2011. október 27.

Magiq Technologies (2007): MAGIQ QPN 8505 Security Gateway. Uncompromising VPN Security (termékspecifikáció) Elérhető: http://www.magiqtech. com/MagiQ/Products_files/8505_Data_Sheet.pdf. Letöltve: 2011. október 27.

Magiq Technologies (2012a): About_Us (weboldal). Elérhető: http: // www.magiqtech.com/MagiQ/About_ Us.html. Letöltve: 2012. augusztus 3.

Magiq Technologies (2012b): Products (weboldal). Elérhető: http://www.magiqtech.com/MagiQ/Products.html. Letöltve: 2012. augusztus 3.

Messmer, E. (2007): Quantum cryptography to secure ballots in Swiss election. Network World (online). Elérhető: http://www.networkworld.com/news/2007/101007-quantum-cryptography-secure-ballots.html. Letöltve: 2011. október 9.

Müller, B. (2009): Code of Silence. Pictures of the Future. 2009 tavasz: p. 50–52.

Póserné Oláh V. (2007): A szervezeti informatikai biztonság megteremtésének, fenntartásának alapvető feltételei. Hadmérnök, II. évfolyam 4. Elérhető: http://hadmernok. hu/archivum/2007/4/2007_4_poserne.html. Letöltve: 2012. augusztus 3.

Quantum Information Partners (év nélkül): State of the Art of Quantum Cryptography today. Elérhető: http://www. qipartners.com/publications/State_of_the_Art_of_ QC.pdf. Letöltve: 2011. október 27.

Quintessence Labs (2012): QuintessenceLabs Inc. – Cyber Defense for the Future Realized Today (weboldal). Elérhető: http://qlabsusa.com/. Letöltve: 2012. augusztus 3.

Schneier, B. (1996): Applied Cryptography Second Edition (elektronikus változat). Elérhető: http://www.cse.iitk. ac.in/users/anuag/crypto.pdf. Letöltve: 2011. április 30.

Szigeti Sz. et al. (2006): Útmutató az informatikai biztonság megvalósítására önkormányzatok számára. Elérhető: http://ekk.gov.hu/hu/eonkormanyzat/letoltes/e_onk_it_ biztonsag.pdf. Letöltve: 2012. augusztus 2.

Verisign (2011): Secure Site Pro with EV (termékleírás). Elérhető: https://www.verisign.com/ ssl/buy-ssl-certificates/extended-validation-pro-ssl-certificates/ index.html. Letöltve: 2011. október 27.

Werlinger et al. (2008): Human, Organizational and Technological Challenges of Implementing IT Security in Organizations. Elérhető: http://lersse-dl.ece.ubc.ca/ record/153/files/153.pdf. Letöltve: 2012. augusztus 2.