Könyvvizsgálati dokumentációk tárolásának biztonságtechnikája / avagy Biztonsági mentések a gyakorlatban, érthetően

Disclaimer: Jelen cikk célja az általános tájékoztatás a biztonsági mentések fontosságáról. A célközönség: az 1-2 számítógéppel rendelkező magánszemélyek és a max 15-20 számítógéppel rendelkező mikrovállalkozások. Természetesen egy 30-50 vagy még több számítógépből álló hálózat esetében egy kis- vagy középvállalatnál teljesen más módszerekkel és technológia felhasználásával történik az adatok biztonságos tárolása. Ha valaki jelen cikk hatására végiggondolja, hogy van-e mentése, mikori mentése van, minden fontos adat benne van-e a mentésében, stb., tehát elkezd, legalább gondolati szinten foglalkozni a témával, akkor a szerző már elérte a célját!

A globalizáció jelensége kihat a társadalmi és gazdasági folyamatokra egyaránt és ennek következtében a világ felgyorsult, a folyamatok automatizálódtak, a digitalizáció a mindennapi élet részévé vált és a mesterséges intelligenciával működő megoldások alkalmazása egyre elterjedtebbé válik. (Hegedűs-Nedelka 2020)

Amikor valaki az adatvédelem szót használja, több mindenre gondolhat. Manapság az “adatvédelem” sokszor a GDPR kapcsán kerül elő, úgy mint “személyes adatok védelme”. Az alábbi sorokban nem erről, hanem az adatok biztonságos tárolásáról lesz szó, melyre inkább az adatbiztonság kifejezés illik jobban. Szintén fontos tisztázni, hogy az adatbiztonságon mit értünk? Egyrészt érthetjük azt is, hogy az adatokhoz illetéktelenek ne férjenek hozzá, másrészt pedig azt, hogy az adatok ne vesszenek el. A továbbiakban az adatbiztonság utóbbi jelentésével, vagyis az adatok elvesztéstől való védelmével fogunk foglalkozni.

Általában is elmondható az adatbiztonság kapcsán, hogy tipikusan “eső után köpönyeg...” jellegű dologról van szó, magyarul mindig sokkal-sokkal olcsóbb előre gondolkozni és kialakítani a biztonsági mentéseket, mint megvárni egy adatvesztést (ami előbb-utóbb mindenképp be fog következni) és akkor próbálni menteni a menthetőt, ami sok esetben nem csak többe (akár nagyságrendekkel többe) kerül, de sokszor egész egyszerűen lehetetlen. Gondoljunk csak egy ellopott vagy elveszített laptopra...

Ismerősöknek szoktam úgy fogalmazni, hogy kollégáimmal “abból élünk, hogy megpróbálunk vigyázni az ügyfeleink adataira”. Ez sokszor, majd látni fogjuk, nem is olyan könnyű feladat.

Gyakran mondjuk: “az az adat, ami csak egy helyen van meg, olyan, mintha meg sem lenne”, magyarul az adatbiztonság ott kezdődik, hogy minden adatnak legalább két, de inkább több adathordozón is meg kell lennie!
Sokszor találkoztam azzal a félreértéssel, hogy “a régi családi fotókról van biztonsági mentésem, mert azokat [csak] egy külső merevlemezen tárolom”. Sajnos mindenkit el kell keserítsek: ha adatokat áthelyezünk egy számítógép merevlemezéről egy külső adathordozóra, azzal csak “áttoltuk a döglött tehenet a szomszéd utcába”, mert ugyanúgy kizárólag egy helyen lesznek meg az adataink, csak máshol. Hasonló a helyzet céges környezetben is, amikor valaki hátra dől, mondván, nála minden rendben van, mert egy NAS-on (hálózati adattárolón) vagy szerveren vannak az adatok. Na jó, de mi lesz, ha azzal az eszközzel történik valami visszafordíthatatlan?

Arra, hogy **az adatok ne csak egy helyen legyenek tárolva**, kézenfekvő megoldásnak tűnik, hogy a számítógépben ne egy, hanem (legalább) két adattároló legyen, melyen tükrözve kerül tárolásra minden adat (un. RAID technológiával), így bármely adathordozó meghibásodása esetén ott a másik és nem vesztünk adatokat. Ez természetesen nagyon jó, de rengeteg esetben nem érünk vele semmit. Ha a komplett géppel történik valami (ellopják, villámcsapás éri, beázik, kigyullad, stb.), elveszett minden adatunk. Ha a tükrözésért felelős komponens megy tönkre, szintén sérülhetnek az adatok, nem beszélve arról, hogy a tükrözés lényege, hogy folyamatosan, minden változást minden lemezre rögzít a rendszer, így például a véletlen felülírásokat, törléseket is. Ezen esetekben sem számíthatunk a tükrözésre a felülírt/törölt adatok visszaállítása érdekében.

A következő, amit tisztázni kell, az a biztonsági mentés és az archiválás közötti különbség. Utóbbi során a cél az, hogy minden adatunk, ami valamikor létezett, "örökre" megmaradjon, tehát egy olyan tárolásról van szükség, ahol azt követően is elérem az adataimat, miután azokat például töröltem.
Egy jól kialakított, "fenntartható" biztonsági mentési stratégia tehát akkor is megvéd minket, ha az élő adatokat tartalmazó adathordozó / számítógép meghibásodik, illetve véd felhasználói hibáktól is (pl. törlés, felülírás, stb.), ám védelme korlátozott, tehát pl. egy törölt fájlt csak egy bizonyos ideig tudok visszaállítani. Ez az időintervallum tolható ki igény szerint a mentésre használt kapacitás növelésével.

Kulcskérdés, hogy mit mentsünk? Ehhez tudnunk kell, hogy hol és milyen, számunkra vagy a cég számára fontos adataink vannak!
Elég egy mappát védeni? A dokumentumok mappát mondjuk? Rendben, de akkor mi van az asztalon tárolt fájlokkal? Mi van a különböző programok által használt adatbázisokkal? Azokat elég egyszerűen, fájlként lemásolni, vagy az adott program beépített mentésével kell kimenteni az adatbázist? A levelezés mentése megoldott a szolgáltató által? A kimenő levelek mentése is? A telefonokon is egyre több adat (fényképek, SMS-ek, stb.) lapul így érdemes azok mentéséről is gondoskodni.
Végig kell gondolni, hogy milyen számítógépeken és milyen eszközökön tárolunk adatokat? A legtöbb cégnél a célravezető az, ha van egy "kiszolgáló" (szerver) gép és csak azon van fontos adat, így elég csak egy mentési rendszert üzemeltetni. Ebben az esetben az egyes kliensgépek "csereszabatosak", tehát bármelyik bármikor elromolhat, "csak" le kell cserélni egy újra, aggódni nem kell, mert adat nem volt rajta.
(Amikor "szerverről" beszélünk informatikai értelemben nem feltétlenül szükséges "igazi szerverre" gondolni, a "központi gép" lehet egy sima számítógép is, megfelelő beállításokkal ellátva.)

A "mit mentünk?" kérdéshez kapcsolódó, eldöntendő kérdés még, hogy elég, ha a rendszerről a fontos adatokat mentjük vagy a komplett rendszert akarjuk menteni inkább, a Windows-zal és a programokkal együtt? Iménti kicsit problémásabb és lassabb, ám egy esetleges meghibásodás esetén lehet, hogy gyorsabb belőle a visszaállás.

A mentés gyakorisága a következő, amit szabályoznunk kell. Lehet folyamatos, óránkénti, naponkénti, heti, havi, stb. Érdemes lehet ezeket kombinálni a cél érdekében, mert bizonyos adatokról elég, ha hetente készül egy mentés, ám fontos fájlok esetében lehet, hogy egy adatvesztés után a 45 perccel korábbi változat sem elég friss...

A fentiekből talán egyértelmű, hogy a jó mentés automatizált, vagyis nem valakinek a dolga, mert az illető elfeledkezhet róla, szabadságon lehet, stb. Murphy szerint pont akkor nem készül majd mentés, amikor fontos lett volna.

Sajnos végtelen kapacitással jelenleg még egyik adathordozó sem rendelkezik, így az adatmennyiségtől függően meg kell hoznunk azt a döntést is, hogy az egyes mentéseket mennyi ideig tároljuk el? A repertoár itt is az egészen egyszerű stratégiától (ti. az elkészült mentéseket X idő után töröljük) a kifejezetten bonyolultakig (pl. napon belül óránkénti, héten belül napi, hónapokon belül heti és hónapokra visszamenőleg pedig havi mentéseket tárolunk el.)

A következő fontos kérdés, hogy hova készüljenek a mentések? A legfontosabb, hogy mentéseket sosem arra a merevlemezre készítjük, amelyen a védendő adatok is vannak! Ez olyan lenne, mintha a kulcsaimról, a biztonság kedvéért készített másolatokat is ugyan azon a kulcscsomón tartanám, mint amin az eredeti kulcsokat.
Triviális megoldás, ami rengeteg esetben teljesen meg is felel a célnak, ha a mentéseket pl. a szervergépre kötött külső merevlemezre készítjük. Baj esetén egy mozdulattal átköthető egy másik gépre és az utolsó mentéstől folytatható a munka, addig is, amíg a szerver javításra nem kerül. Probléma akkor van, ha pl. egy betörésnél nem csak a szervert, hanem a mentési merevlemezt is elviszik a szerverrel együtt…
A mentések készülhetnek un. NAS-ra, ami hálózati adattárolót jelent. Ezt el tudjuk helyezni az iroda egy szervertől (=adatoktól) fizikailag távol eső pontján (pl. konyhaszekrény sarkában), így akkor is védve vagyunk, ha a szerverrel és az elsődleges mentéseket tároló külső merevlemezzel is vis major (betörés, tűz, beázás, stb.) történik.
Még jobb megoldás, ha van un. “off-site” mentésünk is (!), ami azt jelenti, hogy egy mentés nem azon a “földrajzi” helyen van, mint az adataink. Ez lehet havonta a telekre levitt külső merevlemez, ám aki elővigyázatos, az ebből is kettőt tart fent, és hol egyiket, hol másikat hozza fel a telekről a friss mentésre, mert ha a havi mentési művelet során történne valami az adatokkal és a “telki mentéssel” egyszerre, akkor minden elveszne...

Így, a XXI. század elején **a legelterjedtebb “off-site” mentést a felhős rendszerek jelentik**.
A legnagyobb szereplők a piacon a Microsoft és a Google, de Dunát lehet rekeszteni a hasonló felhős tárhelyet kínáló cégekkel. Közös bennük, hogy az előfizetési díjért egy internetes tárhelyet biztosítanak, ami többek között a biztonsági mentések tárolására is alkalmas. Ez remekül véd bármilyen műszaki hiba vagy fizikai megsemmisülés ellen, ám fontos, hogy meg kell bíznunk az adott cégben, hogy a nálunk tárolt adatainkhoz mi és csakis mi férhetünk hozzá. Személyes adatok esetében, a GDPR-nak megfelelően, arra is figyelmet kell fordítanunk, hogy pl. az adott cég szerverközpontja(i) EU-n belül legyenek. Szerencsére a nagyok (Microsoft, Google) ezt biztosítják már számunkra.
A felhős mentés jó szolgálatot tehet egy esetleges titkosító- más néven zsarolóvírus-támadás esetén is, mert bár az automatikus szinkronizáció miatt a vírus által titkosított dokumentumaink a felhőbe is feltöltődnek, ám a legtöbb szolgáltatásban van “időgép” funkció, amivel a teljes felhőnk egy korábbi időpontra állítható vissza.
Sajnos “nem minden felhő bárányfelhő”... A “minden adat legalább két helyen” elv alól a felhős tárolás sem kivétel. A közelmúltban két nagy cég is (Canon, Adobe) vesztette el felhasználók millióinak (!) adatait, így a “kizárólag felhős tárolás” pont olyan, mint a cikk elején említett “biztonságban vannak a fotóim, mert egy külső merevlemezen tárolom őket” hozzáállás: ha csak a felhőben van meg, akkor arról kell biztonsági mentést készíteni…

"Annál, hogy nincs biztonsági mentés, csak az rosszabb, ha azt hisszük, hogy van, de közben nincs!" - szól az általunk szintén gyakran hangoztatott mondás. Ez azt jelenti, hogy a mentéseket időnként ellenőrizni szükséges. Fontos tisztában lenni azzal, hogy egy esetleges hiba során mennyi idő alatt tudjuk visszaállítani az adatainkat, mert adott esetben az, hogy ha több nap, mire helyreáll a rendszer, önmagában is komoly károkat tud okozni akkor is, ha egyébként egyáltalán nem veszett el adat az incidens során. Gondolni kell arra, hogy a mentési terület megtelhet például. Nincs annál rosszabb, amikor egy szerverhiba után eszmél rá az ember, hogy több hónapja nem készült friss mentése, mert elfogyott a mentési tárhely. Ugyan így fontos pl., hogy ha cikk elején említett tükrözéssel dolgozunk, akkor azt is ellenőrizni kell időnként, mert pont az ennek a rendszernek a lényege, hogy ha az egyik merevlemez meghibásodik, abból mi észre sem veszünk semmit, ám onnantól kezdve nincs tükrözésünk és egyetlen lemez működik, ki tudja, meddig. Felhős mentéseknél ugyanígy el tud fogyni a tárhely, ki tud jelentkezni a szinkronizálást végző szoftver, lejár a bankkártya, amivel a havidíjat fizetjük, stb..
Időről időre azt is végig kell gondolni, hogy nem kerültek-e olyan helyre új adatok, melyet nem védünk mentéssel. Tipikus példa, hogy 2020-ban beállítottuk pl. a bérszámfejtő program mentését, de a 2021-es program egy új adatbázisba dolgozik, mely (magától) nem került bele a mentésbe…
Fentiekből egyértelműen látszik, hogy a mentések időről időre történő “kézi” ellenőrzése mennyire fontos részét képezi a biztonsági mentési stratégiának. Sajnos a kényelem és a biztonság egymással mindig ellentétesek: ha valami nagyon biztonságos, az általában nem kényelmes, és fordítva...

A téma kimeríthetetlen, a lehetőségek tárháza korlátlan. Minden mentés jobb annál, mintha egyáltalán nem lenne mentés… Remélem, fenti sorokkal elértem a célom és minden olvasó átgondolja a mentéseinek helyzetét és lépéseket tesz, amennyiben nincs minden megnyugtatóan rendezve nála!

A cikket írta: Tóth Gergely (Expertinit Kft.) rendszergazda. 18 éve foglalkozik kisirodai rendszergazdai tevékenységgel, melynek kiemelt részét képezi az ügyféladatok biztonsági mentésének területe. Elérhetőség: www.bajvan.hu, +36-20-527-8001, bajvan@bajvan.hu

Irodalomjegyzék

1. Hegedűs Mihály, Nedelka Erzsébet: **The impact of digitalization and Industry 4.0 on the audit**, LIMES: A II. RÁKÓCZI FERENC KÁRPÁTALJAI MAGYAR FŐISKOLA TUDOMÁNYOS ÉVKÖNYVE 6: (1) pp. 211-220.