IT BIZTONSÁG KÖZÉPTÁVÚ KIHÍVÁSAI A NAGYVÁLLALATI KÖRNYEZETBEN.

(Váraljai Csaba, Szerencsejáték Zrt.)

2015

SZERENCSEJÁTÉK ZRT.

Váraljai Csaba

Szerencsejáték Zrt.

Információvédelmi Osztály vezetője

- 1980-ban életre szóló fertőzés;
- 1997 óta az IT területen;
- Jelentősebb munkák, és munkakörök;
- 2010 óta a Szerencsejáték Zrt.-nél osztályvezető;
- 10 fő a jelenlegi csoportlétszám;
- 25 perc előadás, 5 perc KF.

SZERENCSEJÁTÉK ZRT.

Mi az IT biztonság?

- Bizalmasság;
- Sérthetetlenség;
- rendelkezésre állás biztosítása.

Bizalmasan kezeljünk olyan „adatokat” amiket a megfelelő módon, és időben biztosítsuk az arra „jogosult felhasználónak és/vagy rendszereknek”, és biztosítjuk őket arról, hogy ez a „adat” az, amit kértek, nem más, és nem más tartalommal.

Milyen adatokról van itt szó?

- Ami fontos;
- Adatvagyonleltár;
- Adatosztályozás.

Első nagy kihívás, A fontos adatok meghatározása!

Ki mondja meg, hogy melyik adat a fontos? Az üzlet, az üzleti folyamat, a Board, a management, a törvények, a szerződött partnereink, aki meg tudják nekünk fogalmazni, mi az ami számukra fontos.

Hogyan kezdjek neki? Az adatvagyonleltár egy olyan táblázat, amiben felsorolom, hogy milyen adataim vannak, és hol tárolom őket.

Milyen adatosztályokat hozzak létre, és mennyit? Amilyet akarok, és amennyi ahhoz kell, hogy a feladatot el tudjam végezni.

Például: Publikus, Alacsony-Alap, Fokozott-közepes, Kiemelt-magas-titkos, +1 Minősített, +2 Államtitok,

Gyakorlatilag a munka 60%-át elvégeztük. Ezek után meghatározom az osztályba sorolás módszertanát, utána meg kell mondani, hogy az egyes osztályokhoz milyen védelmi intézkedéseket társítok, ezeket megvalósítom, és kész.

Hol vannak a kihívások???

- BYOD és a CWiFI;
- Cloud;
- IaaS, SaaS, PaaS;
- ATP, UTM, IDP;
- IDM, AGS, NAC;
- IOT;

BYOD és a CWiFi

- Tényleg kell?
- Mik az előnyök?
- Mik a hátrányok?

Hozd a saját eszközöd! Minek? Hova? Adjam oda a Rendszergazdának a saját laptopom?

„Miért nem lehet a saját okos-telefonomon elolvasni a céges levelezést, azonnal állítsák be.”

Tényleg kell ez egy vállalatnak? Kell, és azért, mert mások is elérik a Cégük bizonyos rendszereit, és ezzel versenyelőnyben kerülnek, mert gyorsabban tudnak reagálni az eseményekre, mint azok, akiknek ez nem biztosított.

Miért jó a saját eszköz? A munkaerő a saját költségein vásárolja meg a szükséges eszközt, és ő maga választja ki, és ÉRDEKLI, és ért hozzá, hiszen maga választotta. Amikor a céges szolgáltatás megjelenik az eszközön, már ismeri az alapfunkciókat, és csak azt kell megtanítani, hogyan használja.

Hátrányok? Nem tudunk semmit, az eszköz és annak szoftvereire vonatkozó biztonsági beállításokról. Titkosítás? Vírusvédelem? Mások is használják? Mi van akkor, ha a BYOD eszköz megváltozik? Hogyan kezeljük a „kezelhetetlen” heterogén rendszerkörnyezeteket?

Cloud - FELHŐ

- Akkor most pontosan mi is a Cloud - FELHŐ?
- A Cloud veszélyei, hátrányai;
- Privát felhő, Hibrid felhő?

Szerintem egy marketing fogás, semmi több. Olyan szolgáltatások összessége, amik már a Cloud megjelenése előtt is léteztek, csak újracsomagolták őket.

„Minden olyan virtualizált környezet, és/vagy azon biztosított szolgáltatások összessége, ahol az erőforrások az igényekhez igazított mértékben állnak a rendelkezésünkre, miközben harmadik félnél van a teljes kontroll és felelősség." Az adataink biztonsága a szolgáltatótól függ, valós biztonság kialakítása körülményes. Minden, amit ebben a környezetben valósítunk meg, csak a szolgáltató minőségén (rendelkezésre állás ugye) múlik. A szerződések igazából nem érnek „semmit" ITB szempontból.

Teljesen virtualizált rendszereket mi is építhetünk magunknak, saját szerverek, saját oprendszerek, saját alkalmazások, saját szerverszoba, saját működési környezet. Ez teljesen új rendszert jelent, A rendszergazdákat át kell képezni, a technológiai feltételeket biztosítani kell ehhez. Ez a Privát felhő. A működési környezet ugyan az, csak a rendszerek feletti kontrol nálunk marad. A hibrid felhő ennek a kettőnek a tervezett „keveréke".

IaaS, PaaS, SaaS

- **I**nfrastructure as a **S**ervice;
- **P**latform as a **S**ervice;
- **S**olution as a **S**ervice.

Ezek voltak a felhő előtti nevei a már említett szolgáltatásoknak. Még mai is elérhetőek ezek a szolgáltatások, de mind egy FELHŐ alapú környezetben, és egy közös szolgáltatói csomag keretein belül. De gyakorlatilag ugyan az.

ATP, UTM, IDP

- **A**dvanced **T**hreat **P**rotection;
- **U**nified **T**hreat **M**anagement;
- **I**ntrusion **D**etection and **P**ervention systems;
- **F**irewall on the **B**ack.

Mindegyik terület nagyon fontos, HA! Van olyan szolgáltatásunk, amit meg kell védeni, és látszik az internet felől. Amennyiben a Társaság IT környezete elérhető az „internet" felől, vagy onnan kap adatokat, akkor valószínűsíthetjük, hogy veszélynek vagyunk kitéve.

Ezek gyakorlatilag célhardverek, célalkalmazások, amik tényleg megbízható és hatékony megoldást nyújtanak bizonyos szolgáltatások védelmére, és bizonyos támadások ellen. **Hátrányuk,** hogy drágák, és komoly szakmai tudást igényel a működtetésük.

Előnyük, hogy arányba hozható a védelem szintje az esetleges károkozás bevételkiesésével.

FOTB egy új megközelítése az ITB logikának. A legfontosabb ITB szabályok, és a biztonsági szakemberek vágyai a tűzfalban van, a rajta futtatott tűzfalszabályok képében. Ha az kompromittálódik, vagy elérhetetlenné válik, akkor minden kommunikáció leáll a „külvilággal".

IDM, AGS, NAC

- **I**dentity **M**anagement;
- **A**ccess **G**overnance **S**ystems;
- **N**etwork **A**ccess **C**ontroll.

IDM. 10 alkalmazottnál és két-három rendszer esetében az IT csapat képes követni a hozzáférések szintjét. Mi a helyzet 100+ alkalmazott 10+ rendszere esetén? Ekkora szervezetnél már van szervezeti felépítés, és vannak munkakörök. Ezekre lehet jogosultsági szabályokat alkotni HA van üzleti folyamattérképünk, adatvagyonleltárunk. Az IDM rendszerek legnagyobb problémája, hogy jól definiált szervezet, és pontos feladatkörök, valamint hozzá tartozó informatikai rendszerek szükségesek, azokon is rendszerszemléletben kialakított jogosultságokkal.

AGS. Vannak rendszereink, van egy rakat felhasználónk, van még több jogosultsági szintünk, és ezeknek követhetetlen számú permutációja. Még ha a dokumentálás, és engedélyezés folyamata ki is van alakítva, akkor is ezeket egyesével leellenőrizni, komoly erőforrás igényes feladat, és nem biztos, hogy ez lenne a rendszergazda legfontosabb feladata. Az AGS képes a felügyelet alá vont rendszereknél a jogosultságok rendszerezett felülvizsgálatára, auditálására, követésére, engedélyeztetésére. Hálózati eszközeink ilyen jellegű nyilvántartását pedig a **NAC** biztosítja számunkra.

IOT

- IOT?
- Mire jó, és mi ezzel a baj?

Az **„Internet Of Things”** igazi kihívás elé állítja az informatikusokat, és a vállalatnak is komoly feladatokat fog generálni a következő években. A dolgok internete az a kommunikációs jelenség, amikor a gépek egymás között, vagy egy központi rendszerrel „beszélgetnek” egymással emberi beavatkozás nélkül.

Nagyon sok mindent el lehet érni az IOT használatával, de egyben ez a legnagyobb hibája is a rendszernek. Gépek adnak át adatokat egymásnak, majd ezek alapján hozzuk meg a döntéseinket, ezek alapján számoljuk, vagy számoltatjuk el a költségeinket, és ezek alapján fogjuk megváltoztatni a gyártási folyamatainkat is.

Ennek a területnek a megfelelő beillesztése a vállalat működésébe elképesztő költséghatékonyságot tud biztosítani. Például: a gyártásban (Just In Time). Gyártás-vezérlés közvetlenül a megrendelések alapján; Gépjárműkövetés, és ez alapján az elszámolás, menetlevél vezetése; „okosmérők”, és „okosfogyasztók”; stb.

ITB szempontból, viszont masszív rémálom ennek a kezelése, a biztonság fenntartása, a központi rendszer védelme.

Dokumentáltság

- Logelemzés;
- Incidenskezelés és változáskezelés;
- Dokumentumkezelés, és verziózás.

Íme minden rendszergazda rémálma az IT apokalipszis négy lovasa. Vagy öt ☺

Logelemzés. Egy ember számára feldolgozhatatlan mennyiségű naplófájl bejegyzés keletkezik egy átlagos munkanapon, akkor is, ha nincs incidens. Mit elemezzek rajta? Mindent? Nem. Csak azt, ami szükséges. Ki mondja meg mi szükséges? Az előadás eddigi részei. Az üzlet, az igény a működésre, és annak jósága.

Incidenskezelés és változáskezelés. Mi az incidens? Minden, amit az üzlet, és az üzemeltetés egyszer kinyilatkozott. És milyen változást kell kezelni? Mindet, amit előírunk, magunknak. Minek? Hogy az üzletmenet folytonosság fenntartható legyen.

Dokumentumkezelés, és verziózás. A nélkülözhetetlen felhasználó, és az emberi kockázatok csökkentésének egyik hatékony módszere. A Rendszeresség és a relevancia biztosíthatósága. A holnapnak dolgozol, nem a mát igazolod.

Van még valami?

- A felhasználók és az ő oktatásuk;
- Kockázatkezelés;
- A vezetőség elkötelezettsége.

Talán a legfontosabb, amit még nem vettünk górcső alá, az pedig **a felhasználó** maga. Ha nem kellően képzett, akkor csak két dolog menthet meg minket egy ITB katasztrófától. A szerencse, és/vagy a diktatórikus rezsim. A legtöbb nagyvállalat a második utat választja. Ez nem a top menedzsment hibája sok esetben, mert a rendszergazda nem tud „vezetőül", a vezető, meg „rendszergazdául" nem beszél. Egy vezető azt látja, hogy milliók kellenének egy eszközre, és nem tudja rendesen elmagyarázni a rendszergazda, hogy pontosan mire kell. **Oktatás.** Mindenkinek, a feladatainak és a tudásának megfelelőt, rendszeresen, a tudásszint visszaellenőrzésével.

Kockázatelemzés. Ezzel lehet megmutatni, hogy egy sérülékenység, vagy egy fenyegetettség bekövetkezése milyen gazdasági kárt fog okozni a társaságnak, és annak mennyi a bekövetkezési valószínűsége. Ha egy vezető számára érthető formában megkapja a megfelelő tájékoztatást, akkor bizony döntenie kell. és a döntés magában hordozza a megvalósulás lehetőségét.

Nagyon fontos a vezetőség elkötelezettsége, hogy akarja azt az informatikai fejlesztést, akarja az új technológiákat, és képes legyen elfogadni, hogy vannak olyan ITB fejlesztések, amiket nem lehet gazdaságossági szempontok alapján vizsgálni, míg más megoldások a biztonság növelése mellett képesek gazdasági hasznot termelni (pl. hatékony nyomtatás, JIT, elektronikus dokumentumkezelés, webáruház védelme)

Gyakorlati példák

- Honlap-vizsgálat(ok);
- Adathordozó(k) elvesztése;
- Személyes adat(ok) védelme;
- Kiber-támadások 2010 óta az SzZrt-nél;
- Tűzfalak, tűzfalak, és tűzfalak;
- Az emberi tényező (Social engineering).

Összegzés

A következő évek nagy kihívásai az új technológiák megjelenése, és azokhoz kapcsolódó vezetői igények, valamint a felhasználók tudása közötti különbségek fogják adni. Ha megfigyeljük a támadások típusait, azt fogjuk tapasztalni, hogy mindig ugyan az a módszer, már lassan 20 éve. A leggyengébb láncszem az ember és az ő hiányos tudása.

Ha szeretnénk egy új technológiát, akkor azt mindig vizsgáljuk meg, gazdaságossági szempontok alapján, és a szükségesség okán is. Kell e a vállalatom üzleti folyamataiba az a technológia, amit a barátom mutatott?

Azzal zárom, amivel elkezdtem.

Bizalmasan kezeljünk olyan „adatokat” amiket a megfelelő módon, és időben biztosítsuk az arra „jogosult felhasználónak”, és biztosítjuk őt arról, hogy ez a „adat” az, amit kért, nem más és nem más tartalommal.

Legyen adatvagyonleltárunk, és adatosztályozási rendszerünk. Működjünk szabályzatok szerint, amik a feladathoz és az élethez van igazítva, nem a vágyainkhoz. A szükséges mértékben dokumentáljunk, és végezzünk kockázatelemzést, hogy felderíthessük a sérülékenységeket, és legyünk tisztában a fenyegetettségekkel.

Ez a legnagyobb kihívás, mert magunkkal szemben kell őket alkalmazni, és nem mutogathatunk egy „láthatatlan támadóra”.

Köszönöm a kitartó figyelmet.