HADMÉRNÖK

X. Évfolyam 1. szám - 2015. március

JÉRI Tamás
jeri.tamas@bv.gov.hu

A KRITIKUS INTERNETES SZOLGÁLTATÁSOK BIZTONSÁGOS ÜZEMELTETÉSE

Absztrakt

A kritikus internetes szolgáltatásokkal szemben alapkövetelmény az állandó rendelkezésre állás biztosítása, a bizalmasság és a sértetlenség fenntartása mellett. Jelen írás azt foglalja össze, hogy a napi üzemeltetési gyakorlatban milyen általános és speciális védelmi intézkedéseket kell, vagy lehet tenni, a kritikus internetes szolgáltatások biztonságos üzemeltetéséhez.

The basic requirement of critical internet services is to ensure constant availability with confidentiality and integrity. This paper summarizes the general and specific security measures for the critical internet services in the daily operational practice.

Kulcsszavak: *Internet, üzemeltetés, biztonság ~ Internet, operation, safety*

BEVEZETÉS

A kritikus internetes szolgáltatások (a továbbiakban: KRISZ) [1] definíciójából és legmarkánsabb tulajdonságából egyenesen következik az a tény, hogy a szóban forgó interneten elérhető kiszolgáló programoknak állandó rendelkezésre állással, ugyanakkor az illetéktelen behatolás(ok) megakadályozásával kell működniük. Ezen feladatok együttes érvényre juttatásához összehangolt, tervezett és szakszerű megoldások foganatosítására van szükség.

A KRISZ folyamatos rendelkezésre állásához nélkülözhetetlen egy hálózati interfésszel és internetkapcsolattal rendelkező hardver, egy stabil, megfelelő erőforrás gazdálkodásra képes operációs rendszer, továbbá a szolgáltatást végző szerverprogram az összes szükséges alrendszerével együtt. A téma feldolgozásánál feltételezem, hogy a hardveres és az infrastrukturális adottságok, valamint szükségletek 100%-ban, azaz teljes mértékben biztosítják a rendszer működését, megjegyezve, hogy ezen feltételezés megvalósítása természetesen csak igen nagy ráfordítással érhető el és önmagában is kutatásra érdemes. A szoftveres elemekre szűkítve tehát a KRISZ működését, kiemelkedő fontosságú az operációs rendszer-, valamint az általa vezérelt - hálózatról elérhető, illetve zárt - szolgáltatások kiegyensúlyozott, összehangolt működése. Dolgozatom témája a KRISZ biztonságos üzemeltetése, ezért a hétköznapi gyakorlatból kiindulva vizsgálom, hogy mi vezethet a KRISZ üzemképtelenségéhez? A következőkben e szemléletet követve részletezem a KRISZ biztonságos üzemeltetéséhez szükséges teendőket.

OPERÁCIÓS RENDSZER ÜZEMELTETÉSE

Az operációs rendszer [2], mint a számítógép hardverével közvetlen kapcsolatban álló alapprogram, teret biztosít a végrehajtandó, vagy végrehajtás alatt álló szolgáltatások számára. Az összes felhasználói program felett áll, képes azok indítására, megszakítására, leállítására, tehát egyszerűen képes a beavatkozásra. Napjaink szolgáltatás orientált operációs rendszerei jogosultsági szintekkel rendelkeznek, melyben a hierarchia csúcsán álló kiemelt felhasználó a rendszer működésével kapcsolatos minden folyamatra ráhatással lehet.

A kritikus internetes szolgáltatás is, mint bármely más folyamat teljesen alárendelt és kiszolgáltatott az operációs rendszernek, ezért úgy kell megszervezni az operációs rendszer üzemeltetését, hogy az lehetőleg ne kerülhessen illetéktelen "kezébe".

Behatolás megelőzés

Tekintettel arra, hogy a KRISZ biztosan egy internetről elérhető szolgáltatás, egyértelmű, hogy annak operációs rendszere közvetett kapcsolatban van a világhálóval. Ahhoz, hogy az operációs rendszer ne kerülhessen illetéktelen irányítása alá, meg kell előzni a behatolást. Az internetről az operációs rendszerhez a szolgáltatások csatornáin keresztül vezet az út, ezért a nyitva hagyott hálózati portok számát a minimálisra kell csökkenteni. Egy frissen telepített operációs rendszer indításakor alapértelmezésben is számos hálózati szolgáltatás aktivizálódik, amelyek adott esetben feleslegesen kínálnak hálózati csatornákat a rossz szándékú felhasználóknak. Mivel minden hálózati szolgáltatás üzemeltetése biztonsági kockázat, a feleslegeseket ki kell kapcsolni, ezáltal erőforrás takarítható meg és csökkenthető a támadási felület.

A biztonságos üzemeltetés, így a hálózati szolgáltatások védelme érdekében erősen ajánlott tűzfal alkalmazása, amely többféle szempont szerint képes szűrni a hálózati adatforgalmat. Alkalmazástól függően többféle lehetőség kínálkozik a védelem megteremtésére, mégis célszerű reagáló képesség szerint rendszerezni a tűzfalak viselkedését.

Statikus tűzfal

A tűzfalak mechanizmusa egyrészt a csomagszűrésen (packet filter), másrészt az alkalmazási átjárón (application gateway) alapszik. Míg az előző az áthaladó csomagokat a forrás és a cél IP[1] cím, illetve hálózati port szerint vizsgálja és dönt azok további sorsáról, addig az utóbbi a csomagok összeállását követően, az üzenet mérete vagy tartalma szerint engedélyezi, vagy tiltja a hálózati forgalmat. [3]

A tűzfal működését alapvetően az előre rögzített tűzfal-szabályok befolyásolják, amelyek a tartalom "értelmezése" szempontjából részben tekinthetők dinamikusnak is, azonban a szabályok bővítése, vagy változtatása aspektusából teljesen statikusak, váratlan eseményre nem képesek reagálni.

Dinamikus tűzfal

"A tűzfal alapötlete az, hogy megakadályozza a támadók be-, valamint a titkos adatok kijutását. Sajnos vannak azonban olyan emberek is, akiknek nincs jobb dolguk, mint hogy megpróbáljanak egyes helyeket térdre kényszeríteni. Ezt úgy érik el, hogy olyan nagy számban zúdítják az egyébként legális csomagjaikat a céljukra, hogy az összeomlik a terhelés alatt." [3]

Számos olyan szituáció létezik, amikor az előre megírt, egyébként a céljuknak teljesen megfelelő tűzfal szabályok nem képesek reagálni olyan eseményre, amely a KRISZ működését - könnyen - negatívan befolyásolhatja, vagy gátolhatja.

A próbálgatás (brute force[2]) alapú, vagy a szolgáltatás megbénítására irányuló (DoS[3], DDoS[4]) támadásokra megoldást jelenthet a napló állományok elemzése alapján, dinamikusan módosuló tűzfal szabályok alkalmazása. A reagáló képesség lényege, hogy az operációs rendszer állandó háttérfolyamataként egy program [4] vizsgálja és analizálja a megjelölt napló állományokat, majd annak tartalma szerint, előre rögzített eseményekre (pld. meghatározott időn belül túl gyakori kapcsolat létrehozás kérése) az előző pont szerinti statikus tűzfal szabályt aktivál, illetve a biztonság helyreállása esetén in-aktivál.

Rendszergazdai feladatok ellátása

Az operációs rendszereket időnként karban kell tartani, felhasználói hozzáféréseket kell kezelni, állományműveleteket kell végezni. A gyártók folyamatosan biztosítják a frissítő-, karbantartó csomagokat, amelyek - általában - a felfedezett programhibák és biztonsági rések javítását szolgálják és telepítésük erősen ajánlott. Kérdés, hogy az operációs rendszert üzemeltető rendszergazda milyen eljárással kívánja az adminisztrációs feladatokat végezni? Egyik lehetőség, hogy a szerverrel megteremti a fizikai kontaktust, amely - tekintettel arra, hogy az operációs rendszer kapcsolatban áll az internettel - valószínűleg több-kevesebb utazással jár, vagy kialakítja a távoli adminisztráció lehetőségét. Az utóbbi kézenfekvő megoldás, viszont egy plusz szolgáltatás fenntartásával és egy újabb kockázat viselésével jár, hisz behatolásra ad lehetőséget.

Távoli shell

Távoli shell-ként a továbbiakban azt a hálózaton keresztül elérhető parancsértelmezőt értem, amely az adott operációs rendszer típusától függetlenül, lehetőséget ad az operációs rendszerbe történő belépésre, majd ott - jogosultság és parancsértelmező függvényében - utasítások végrehajttatására.

---

[1] Internet Protocol - Internet Protokoll
[2] nyers erő
[3] Denial of Service - szoláltatásmegtagadással járó támadás
[4] Distributed Denial of Service - elosztott szoláltatásmegtagadással járó támadás

A távoli elérés biztosításának és a megfelelő védelem kiépítésének problematikája sajnos megkerülhetetlen, mert a szolgáltatás fenntartása és a biztonságos üzemeltetés egymással ellentmondásban vannak, hisz

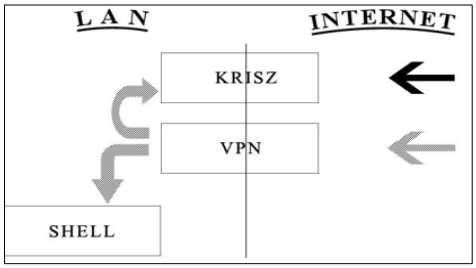
- az operációs rendszer és a telepített programok normális működése esetén a távoli shell egy "szükségtelen alkalmazás", mert biztonsági kockázatot jelent és fogyasztja az erőforrásokat;
- bármilyen operációs rendszer-, vagy szoftver-szintű probléma esetén a távolis shell az elsődleges megoldás a beavatkozásra, hiányában utazni kell a szerverhez.

Alapvetően a távoli shell kiszolgálója egy biztonságos, titkosított csatornán ad lehetőséget a hozzáférésre, ugyanakkor próbálgatással, akár brute-force módszerrel előbb-utóbb - főleg gyenge jelszavak esetén - mégiscsak be lehet jelentkezni az operációs rendszerre, továbbá a próbálgatások kiszolgálása erőforrás vesztéssel és felesleges energia felhasználással jár.

Az ellentmondás feloldására megoldást jelent(het) a távoli shell - szükség szerinti, - interneten keresztül történő ki-be kapcsolásának a lehetősége. [5] A KRISZ feltételezhetően rendelkezésre fog állni, hisz az erőfeszítések alapvetően annak működése érdekében történnek, így lehetőséget adhat arra, hogy egy előre programozott metódussal és a szükséges jogosultságok érvényesítésével a távoli shell ki-be kapcsolása megtörténhessen. Alkalmazásával a rendszeradminisztrátori feladatok biztonságosan végezhetők.

Virtuális magánhálózat (VPN) használata

"... a VPN-ek (Virtual Private Networks - virtuális magánhálózatok) a nyilvános hálózatok tetejébe épülnek, mégis rendelkeznek a magánhálózatok legtöbb tulajdonságával." [3] A VPN adta lehetőségeket kiválóan ki lehet használni a KRISZ-el kapcsolatos üzemeltetési feladatok biztonságának növelése érdekében. Az alap koncepció szerint, a KRISZ szerverét el kell látni plusz egy belső, internet előtt rejtett IP címmel, továbbá egy biztonságos VPN csatornát kell kiépíteni az internethez kapcsolódó interfészen keresztül. A virtuális magánhálózat csatornáján, a belső rejtett IP címhez kapcsolódva el lehet végezni azokat az üzemeltetési feladatokat, amelyek közvetlen internetes felületen keresztül kiemelten nagy kockázattal járnának (1. ábra).



1. ábra. VPN működtetése interfészek szerint

A VPN-en keresztül biztonságosan elérhető az előző pontban ismertetett távoli shell is, továbbá a KRISZ alrendszereként [6] működő adatbázis-kezelőhöz is e titkosított csatornán keresztül ajánlott a közvetlen csatlakozás.

Helyreállítás biztosítása

A KRISZ működését biztosító operációs rendszeren elengedhetetlen ütemezetten mentéseket végezni, melynek magában kell foglalnia az operációs rendszer, valamint a KRISZ teljes értékű helyreállításához szükséges adatokat. Nem várt esemény bekövetkezése esetén, a mentésből - minimális veszteséggel - visszaállíthatók azok az adatok, amelyek a rendszer újraindításához, ismételt működéséhez szükségesek. Az automatizált, rotációs rendszerű archiválások a legcélszerűbbek, amelyek lehetnek növekményes alapon, vagy mindenre kiterjedően szervezettek. Az archívumokat célszerű úgy tárolni, hogy azok bármikor rendelkezésre álljanak, ugyanakkor védettek legyenek a külső környezeti hatásoktól.

KRISZ ÜZEMELTETÉSE

A KRISZ, mint kiemelt szolgáltatás üzemeltetésénél, a hangsúlyok részben eltérnek az operációs rendszernél megfogalmazottaktól, amelynek legfőbb oka a közvetlen internetes elérés. A biztonságos üzemeltetéshez legfőképpen az árulkodó információk elrejtésére és a felesleges támadási pontok megszüntetésére van szükség.

Érzékeny információk elrejtése

Függetlenül attól, hogy a KRISZ Web[5], Mail[6], FTP[7], vagy egyéb kiszolgálásra irányul, kerülni kell, hogy a szerverprogram önmagáról, vagy alrendszereiről felesleges - kompromittáló - információkat adjon ki. A fejlesztők gyakran alapértelmezésként úgy konfigurálják ezen programokat, hogy azok a kapcsolódásnál önmagukról és néha még az operációs rendszerről is minden, típussal és verziószámmal kapcsolatos információt kiadjanak. Természetes, hogy a támadó a szolgáltatás "térdre" kényszerítéséhez elsősorban pontosan azokat az információkat szeretné beszerezni, amelyek a támadás előkészítéséhez szükségesek. A programok hibáiról, gyengeségeiről, támadhatóságáról - gyakran az interneten is - fellelhető tudásbázisok rendezési elve, pontosan a programok típusára és verziószámára irányul, ezért a "tálcán kínált", - ismert - biztonsági réssel működő szolgáltatások kitettséget jelentenek a rossz szándékú internet használók felé. Ezért azon - alapértelmezett - beállításokat ki kell iktatni, amelyek a kiszolgáló programról, vagy az operációs rendszerről árulkodó információkat közölnek.

A Web alapú KRISZ gyakran olyan összetett szolgáltatás, amikor a felhasználó felé közvetített információ HTTP[8](s) protokollra ültetve, programozott módon, adatbázisból származtatva, interaktívan kerül előállításra. A Web népszerűségéből adódóan, az előre elkészített - tartalomkezelő - programok nagy számban jelentek meg, amelyek web-kiszolgálóra telepített használata közkedvelt, olcsó és KRISZ-ként is használható. Számos esetben ezek a Web-es rendszerek programozási hibákat, így támadható pontokat is tartalmaznak, ezért kiemelt fontosságú, hogy ne adjanak önmagukról a gyártóra, a verzióra, a mögöttes adatbázis-kezelőre, vagy az operációs rendszerre vonatkozóan információkat. Az árulkodó információk elrejtése az üzemeltető feladata, amely a legtöbb esetben programozási gyakorlatot feltételez.

KRISZ karbantartása

Mint bármely szolgáltatást, időközönként a KRISZ-t is karban kell tartani, amelynek az operációs rendszer-, a kiszolgáló-, vagy a mögöttes információhalmaz változása egyaránt oka lehet, ezért meg kell teremteni a lehető legegyszerűbb, ugyanakkor kellően biztonságos adminisztrációs feltételeket. A KRISZ karbantartására az adminisztráció jellegétől függően, általában három ponton nyílik lehetőség.

Operációs rendszeren keresztül

A lehető legmagasabb jogosultsági szintű beavatkozást biztosítja, amely a KRISZ bármely pontjának megváltoztatására alkalmas. Használata általában a legmélyebb - akár operációs rendszer közeli - összetevők módosítása esetén (pld. programfrissítés) ajánlott, amelyhez az 1.2 pontban részletezett hozzáférések biztosítása elengedhetetlen. Amellett, hogy ez a módszer a lehető legnagyobb mozgásteret biztosítja a szolgáltatás karbantartására, fontos kiemelni, hogy illetéktelen "kézre kerülése" esetén a KRISZ-re korlátlan csapás mérhető, tehát ezen karbantartási felület fenntartása veszélyes.

---

[5] World Wide Web - világháló
[6] e-mail - elektronikus levelezés
[7] File Transfer Protocol - állomány átviteli protokoll
[88] HyperText Transfer Protocol

Adatbázis-kezelőn keresztül

Az adatbázis-kezelők szerepe [7] kiemelt fontosságú a KRISZ működésében, hisz az adatbázisban tárolt adatok gyakran a szolgáltatás működésének alapját jelentik. Példaként említve a fájl-cserélő, mint KRISZ azon esetét, amikor a felhasználók, valamint a konfiguráció minden paramétere adatbázisban kerül tárolásra, a szolgáltatás karbantartása az adatbázis-kezelő adminisztrálásával - is - megoldható. Ez esetben az internet adta lehetőséggel élve, az adatbázis-kezelőhöz - a lehető legkisebb biztonsági kockázattal - adminisztrációs felületet szükséges biztosítani. Kifejezetten veszélyes az adatbázis-szerver közvetlen internetes elérhetőségének biztosítása, inkább javasolt valamely közvetett - például Web-es, vagy VPN-es - hozzáférés megvalósítása. Illetéktelen hozzáférése esetén a KRISZ fájl-cserélő alapfunkciója kevésbé sérülhet, viszont - a felhasználói adatok kiszolgáltatottsága miatt, - a szolgáltatás alaprendeltetése meghiúsulhat, ezért célszerű és indokolt az adminisztrációs felülethez tartozó hozzáférési pontot rejtve tartani.

KRISZ adminisztrációs felületén

A KRISZ saját kiszolgálóján keresztül gyakran adminisztrálható is, amely meglehetősen kényelmes és kézenfekvő megoldás. Alapkövetelmény, hogy az adminisztrációs felület használatához csak valamilyen további jogosultság rendelkezésre állása esetén legyen lehetőség, illetve, hogy a sikeres bejelentkezéskor minden szükséges karbantartási eszköz elérhetővé váljon. A hozzáférési pont ismerete és a bejelentkezés sikeressége egyben az adminisztráció végrehajtásának a kulcsa.

Web-es szolgáltatás esetén gyakori beállítás, hogy az elérhetőség URL-jéhez egyszerűen hozzáillesztésre kerül az alapértelmezett "/admin" hivatkozás, amely ismeretében a felhasználó belépési lehetőséget kap az adminisztrációs felületre (pld. "http://www.kriszem.org/admin"). Nagy felelőtlenség és egyben komoly kockázatot hordoz magában az adminisztrációs bejelentkezési felület nyílt felajánlása, hisz a rossz szándékú felhasználó próbálgatással, vagy SQL Injection[9] típusú támadással adminisztrációs felülethez-, és jogokhoz juthat, amellyel a KRISZ működésében beláthatatlan károkat okozhat.

Kiemelten fontos tehát, hogy az adminisztrációs felület hozzáférése rejtett maradjon, ezért olyan, lehetőleg egyedi elérhetőséget kell beállítani - a "/admin" URL helyett -, amelynek kitalálása nagy energiát és sok időt követel meg a rossz szándékú felhasználótól. Fontos továbbá, hogy az adminisztrációs felülethez - akár kikényszerítetten - csak titkosított csatornán keresztül lehessen eljutni (pld. HTTPS protokoll), továbbá, hogy a bejelentkezési pont az Injection típusú támadásra ellenálljon.

ÖSSZEGZÉS, KÖVETKEZTETÉSEK

Dolgozatomban a KRISZ gyakorlatból vett - megkerülhetetlen - üzemeltetési feladatainak bemutatásán keresztül, kísérletet tettem annak prezentálására, hogy miként lehet a távoli elérés mellett a szükséges biztonságot fenntartani. Természetesen a biztonságot a fent leírtakon túl számtalan megoldással lehetne még növelni, ugyanakkor igyekeztem azokat az alapokat lefektetni, amelyek betartásával a kockázatokat elviselhető szintűre lehet csökkenteni. Le kell szögezni, hogy néha a legtökéletesebb üzemeltetési praktikák sem nyújtanak segítséget, mert nem védenek a szerverhez fizikailag hozzájutó támadóval-, a szolgáltatás megbénítására irányuló zombie hálózattal-, valamint KRISZ-ben, vagy annak alrendszerében rejlő programhibákkal, hátsó ajtókkal szemben.

[9] kód injektáló technika

Felhasznált irodalom

[1] Jéri Tamás - Kritikus Internetes Szolgáltatások
Hadmérnök, VIII. Évfolyam 1. szám 2013. március, NKE Budapest, ISSN 1788- 1919
http://hadmernok.hu/2013_1_jerit.pdf - letöltve 2014.01.25

[2] Andrew S. Tanenbaum - Albert S. Woodhull: Operációs rendszerek 2. kiadás, ISBN 978-9-635454-76-1 Panem Könyvkiadó Kft., Budapest 2007.

[3] Andrew S. Tanenbaum: Számítógép-hálózatok, ISBN 963 545 384 1,
Panem Könyvkiadó Kft., Budapest 2004.

[4] Fail2ban
http://www.fail2ban.org/wiki/index.php/Main_Page - letöltve 2014.01.25

[5] Jéri Tamás - Számítógép-hálózatok támadása és védelmének lehetséges módszerei Zrínyi Miklós Nemzetvédelmi Egyetem, Diplomamunka, 2010.

[6] Jéri Tamás - A kritikus internetes szolgáltatások alrendszerei, Társadalom és Honvédelem, 2013/3-4. szám, NKE Budapest, ISSN 1417-7293

[7] Jéri Tamás - Az adatbázis-kezelők szerepe a kritikus internetes szolgáltatásokban
Hadmérnök, X. Évfolyam 1. szám 2015. március, NKE Budapest, ISSN 1788- 1919