



## Rendszer-felülvizsgálat

**Az informatikai rendszerek folyamatos külső és belső fenyegetettségnek vannak kitéve. Ezek a fenyegetettségek irányulhatnak a rendszer üzem- és adatbiztonsága ellen.**

Örök érvényű mondás, hogy a rendszer biztonságának az alapja it a tervezésnél rakják le. Ez természetesen nem jelenti azt, hogy elegendő csak a tervezésnél foglalkozni a biztonsággal. Az informatika rendszerek életciklusának minden egyes szakaszában kiemelt szerepe van a rendszer biztonságára irányuló tervezésnek és ellenőrzésnek. A tervezési és fejlesztési szakaszban inkább szakértői tevékenységről beszélhetünk, a megvalósítási, működtetési és leállítási szakaszban pedig rendszer felülvizsgálatról.

Az **Andrews Kft.** több éves gyakorlattal rendelkezik mindkét területen.

Egy rendszer biztonsági felülvizsgálatánál az első lépés a vizsgálat tárgyának pontos meghatározása, a második pedig a megfelelő vizsgálati módszer kiválasztása.

Vizsgálat tárgya	Javasolt vizsgálati módszer
Hálózati architektúra	Security Auditing,
biztonsági felülvizsgálata	Penetration Testing
Szerverek és tűzfalak	Security Auditing, Vulnerability Scanning, Penetration Testing
felülvizsgálata	
Szoftverek biztonsági auditja	Security Auditing, Vulnerability Scanning
Szabályzás felülvizsgálata	Security Auditing

**Az általános sebezhetőség egy olyan állapot a számítógépes rendszer(ek)ben, amikor:**

- ➔ a támadó parancsot tud végrehajtani más nevében,
- ➔ a támadó elérhet olyan adatokat, amelyet az adata vonatkozó hozzáférés szabályozás szerint nem érhetne el,
- ➔ a támadó másnak adhatja ki magát,
- ➔ a támadó DoS támadást intézhet.

Forrás: <http://www.cve.mitre.org/about/terminology.html>

### Vulnerability Scanning (Sebezhetőség-vizsgálat)

A Vulnerability Scanning feladata a rendszerben lévő ismert hibák felderítése. Ezt a feladatot általában automata eszközök végzik, melyek az adatbázisukban található hibaleírások alapján különböző tesztekkel végzik el a rendszeren. Ez jóval több, mint egy egyszerű portscan (port letapogatás), mivel az adott szolgáltatást protokoll szinten próbálják elemezni.

#### Előnyei:

- ➔ meglévő, akár ingyenes eszközöket is lehet használni az elvégzésére
- ➔ gyors
- ➔ nem igényel nagy szakértelmet

#### Hátrányai:

- ➔ nagyrészt csak az ismert programhibák detektálását végzi (az ismertek közül azokat, amikre fel van készítve)
- ➔ sok esetben felületes vizsgálat
- ➔ általában könnyű megtéveszteni (sok esetben elegendő a vizsgált rendszer néhány paraméterét módosítani)

### Penetration Testing (Behatolás vizsgálat)

A Penetration Test esetén a rendszer biztonságának a vizsgálata túlmegy a lehetséges hibák felderítésén. A cél a rendszer kompromittálása. A kompromittálás itt egy megadott (a megbízó által kitűzött) cél megvalósítása, ami például lehet egy állomány elérése egy belső rendszeren, vagy új felhasználó felvétele.

Az alkalmazott módszer célja a valós körülmények szimulálása (mi lenne, ha egy igazi támadó próbálna elérni az adott célt). Az módszer eredménye igen kétséges, mivel a sikertelen próbálkozás sokszor annak tudható be, hogy bizonyos technikákat nem vethet be a tesztelő egy éles rendszeren, míg a támadót nem kötik szerződésben leírt kötelezettség-vállalások.

A Penetration Test esetén a tesztelőnek nem célja az összes hiba felderítése, hanem csak egyetlen, kihasználható hiba keresése. Tehát amennyiben a Penetration Test eredménytelen volt, még nem lehetünk biztosak rendszerünk biztonságában.

#### Előnyei:

- ➔ valós támadást szimulál

#### Hátrányai:

- ➔ nem fedi fel a rendszer minden hiányosságát
- ➔ időigényes



- költséges
- a negatív eredmény nem jelent bizonyosságot a rendszer feltörhetetlenségére
- az éles rendszeren végzett vizsgálat károkat, kiesést okozhat

### Security Auditing (Biztonsági Audit)

A Security Audit a rendszer teljes körű átvizsgálását jelenti. Ebben az esetben a megbízó teljes körű hozzáférést ad az auditot végzőnek a rendszerhez, valamint a rendszerhez tartozó dokumentumokhoz. Az vizsgálat nem áll meg az első megtalált hibánál, hanem a rendszer összes hátulütőjét megpróbálja feldehíteni, a teljes kép ismeretében.

Az audit a következő elemekből állhat:

- teljes körű operációs rendszer audit (beállítások, jogosultságok, verzió frissesség, stb.)
- használt alkalmazások, alrendszerek auditja (konfiguráció ellenőrzés, szükség esetén forráskód elemzés)
- rendszerek közötti bizalmi viszony (trust relationship) vizsgálata
- dokumentáció, szabályzat felülvizsgálata

#### Előnyei:

- a rendszer minden hibája, hiányossága feltárható
- az auditor által adott értékelés a rendszerrel kapcsolatos megrendelői elvárások ismeretében születik

#### Hátrányai:

- időigényes
- költséges
- magas fokú szaktudást igényel

#### Ethical hacking:

- Napjaink felkapott kifejezése (buzzword). Gyakorlatban a Vulnerability Scanning és a Penetration Testing keveréke, de bármi mást is beleérthet a végzője.

### Hálózati architektúra biztonsági felülvizsgálata

Hazánk informatikai fejlődésének jellegéből adódóan számos szervezet belső hálózata evolúciós úton fejlődött. Amennyiben a hálózat tervezése elmaradt, vagy az igények időközben megváltoztak, akkor gyakran előfordul, hogy a belső hálózatokban lehetetlen megfelelő módon biztosítani a különböző biztonsági szintű rendszerek megnyugtató elkülönítését, a hozzáfé-

rés igényeknek megfelelő szabályozását. Az **Andrews Kft.** kiemelkedő tapasztalatokkal rendelkezik országos és nemzetközi kiterjedésű hálózatok védelmi rendszereinek tervezésében, kivitelezésében és üzemeltetésében. A hálózat felépítése és a biztonsági szintek felmérése után szükség esetén javaslatot tesz a hálózat átalakítására, a külső és belső védelmi rendszerek kialakítására illetve módosítására és igény szerint el is végzi a szükséges módosításokat, fejlesztéseket.

### Szerverek és tűzfalak felülvizsgálata

Nagyszámú telepített rendszere építése során, az **Andrews Kft.** hatalmas gyakorlati tapasztalatra tett szert az IT biztonság terén. Szakértői feltárják a szervereken és védelmi rendszereken a lehetséges támadható pontokat, üzembiztonsági hiányosságokat és javaslatot tesznek a lehetséges javításra vagy igény szerint el is végzik azokat.

### Szoftverek biztonsági auditja

Egy programrendszer biztonsága nagymértékben függ annak tervezési koncepciótól, a fejlesztők felkészültségétől, valamint a fejlesztés utáni funkcionális és biztonsági tesztek alaposságától. Sok esetben ezek egy része nem kap megfelelő hangsúlyt, így a rendszer biztonsági vagy üzembiztonsági szempontból több ponton nem felel meg a Megrendelő igényeinek. Az **Andrews Kft.** fejlesztői képesek igény szerinti mélységben átvizsgálni egyedi fejlesztésű vagy nyílt forráskódú szoftverek forráskódját, ezzel nagymértékben növelve annak biztonságát.

A rendszer utólagos funkcionális és biztonsági tesztelése is igen jó megbízhatósággal tárja fel az esetleges hiányosságokat. Érdemes azonban előre tisztázni: amennyiben a program koncepcionális tervezési hiányosságokat tartalmaz, akkor a teljes biztonságot csak szoftver adott részének újratervezése és újrafelkészítése oldja meg. A felmerülő hibák jelentős része általában utólag is javítható, erre igény esetén az **Andrews Kft.** munkatársai javaslatot is tesznek illetve megvalósítják a szükséges módosításokat.

### Szabályzás, dokumentáció felülvizsgálat

Magyarországon a nagyobb cégek többsége rendelkezik az informatika biztonságra vonatkozó szabályzással (IBSZ) és szinte minden cég rendelkezik valamiféle dokumentációval a saját rendszeréről. Mivel a cégek életében az informatikai rendszer folyamatosan változik és megújul, ezért a szabályozásokat és a rendszer dokumentációkat felül kell időnként vizsgálni, különben elavulttá válhatnak. Az ebből adódó veszélyek addig láthatatlanok maradnak, amíg nem történik valami probléma, amiből kifolyólag például egy több éves gépkönyv alapján kell újraépíteni a rendszert.



## Határvédelmi megoldások

**Az IT biztonság nem csupán a felhasznált eszközök összessége, hanem folyamat, melynek kialakításához és fenntartásához megfelelő szakértelemre és megfelelő képességekkel/tudással rendelkező eszközökre van szükség. Az IT biztonság kiemelten fontos területe a hálózati határvédelem, mely feladata a védett hálózatok forgalmának ellenőrzése, a lefektetett szabályok és jogosultságok betartatása, a hálózati forgalmak bizalmosságának és sértetlenségének biztosítása és ellenőrzése, valamint a hálózati események naplózása.**

Az **Andrews Kft.** határvédelmi eszköze egy moduláris felépítésű rendszer, amely képes futni bármely, Linux által támogatott hardveren. A különböző védelmi funkciókat ellátó modulok egymástól függetlenül telepíthetők, hangolhatók és egymástól szeparáltan futnak.

Az alaprendszer rugalmasságából adódóan a rendszer képes akár tíznél több fizikai interface (a hardverkiépítés-függő), valamint több száz virtuális interface és VLAN kezelésére. Teljes körű IPv4 és IPv6 támogatással rendelkezik, és képes kihasználni a gépben lévő több processzort is, nem okoz problémát a gigabites hálózatok kiszolgálása sem. Nagy teljesítményi és/vagy rendelkezésre állási igény esetén a rendszer klaszterezhető aktív-aktív és aktív-passzív módon is.

A következő védelmi modulok állnak rendelkezésre:

- ALF
- VPNgw
- MAILgw
- WEBgw
- QoS
- IDS
- ALF

Az **ALF** az erős és mégis kényelmesen használható hálózati határvédelem eszköze.

Tulajdonságai úgy kerültek kialakításra, hogy a hálózatok gyakrabban használt szolgáltatásain a lehető legszélesebb körű védelmet nyújtsa a támadók ellen. Fejlett naplózó és azonosító alrendszerei segítségével hatékony eszközt biztosít a védett hálózatokhoz történő hozzáférés kialakításához és az itt történt események elemzéséhez.

Rugalmas felépítésének köszönhetően az ALF egyaránt alkalmas kis és nagy méretű – különböző biztonsági szintű – hálózatok, valamint kliensek és szerverek hatékony védelmére. Moduljai finoman szabályozhatók, ezáltal könnyen alakítható egyedi igényeknek megfelelően. Széleskörű kompatibilitásának köszönhetően könnyen illeszthető már meglévő – heterogén – hálózati környezetbe.

### MAILgw

Az Internet kapcsán az egyik legismertebb szolgáltatás az elektronikus levelezés. Napjainkban a cégek működése már elképzelhetetlen gyors és megbízható üzenetváltások nélkül. A levelezés népszerűsége, hasznossága mellett komoly biztonsági, működési kockázatokat rejt. A legfrissebb adatok alapján a levélforgalom közel 95% kértelen levelekből (SPAM) áll, és a vírusok egy része is leveleken keresztül terjed.

Az **Andrews Kft.** által használt MAILgw szolgáltatás biztosítja, hogy a levelek biztonságosan célba érjenek. Hatékony, naprakész víruskereső szolgáltatása révén védelmet biztosít a belső infrastruktúra számára. A SPAM-ek elleni védelem alapja egy nagyon jól hangolható szűrő, amely már a levél fogadása során megakadályozza, hogy a felhasználó postafiókjába kértelen levelek juszanak. A rendszer folyamatosan tanul, illetve a felhasználók által tanítható, így még erőteljesebben lehet fellépni a levélszeméttel szemben. A cég előírásának megfelelően lehetőség van a levél paramétereire, a csatolmányok formátumára is szűrni.

A MAILgw szolgáltatás egyszerűen beilleszthető egy már meglévő levelezőrendszer elé, így nem igényel komolyabb migrációt a használata, illetve a felhasználók beállításain sem szükséges változtatni.



## VPNgw

A legtöbb forgalom titkosítás és azonosítás nélkül zajlik a hálózatok használata során. „Szakértő kezek” ezeket a forgalmakat könnyedén lehallgathatják és módosíthatják, így kényes adatokhoz jutnak a cég működésével kapcsolatban, amely akár komoly anyagi következményekkel járhat.

Az **Andrews Kft.** által használt VPNgw szolgáltatás lehetőséget biztosít, hogy a forgalmak megfelelő titkosítás, ellenőrzés mellett érjenek célba. Segítségével költséghatékony magánhálózatokat hozhatók létre távoli telephelyek között. A telephelyeken dolgozó felhasználók különleges beállítások nélkül érhetik el az erőforrásokat.

Gyakran felmerülő igény, hogy partnereknek, dolgozóknak a cég távolról is ellenőrzött, titkosított kapcsolatot biztosítson. A VPNgw erre több megoldást kínál. A napjainkban használt operációs rendszerek által ismert kliensek segítségével biztonságosan férhet hozzá a cég belső erőforrásaihoz. Természetesen ebben az esetben is a céges előírásoknak megfelelő engedélyek vonatkoznak a kapcsolatra.

A VPNgw a legelterjedtebb gyártók hasonló termékeivel kompatibilis, a jelenlegi biztonsági normáknak megfelelő algoritmusokat támogatja.

## WEBgw

A webserverek üzemeltetése során a megbízhatóság mellett gyakran felmerülő igény a nagyobb sebesség, illetve a terhelés ésszerűbb elosztása.

Az **Andrews Kft.** által használt WEBgw szolgáltatás a webserverek elé épül be, és kiszolgálja a klienseket. A statikus tartalmakat (pl. képeket, szövegeket, videókat) gyorsítótárból szolgáltatja, így komfortosabbá téve a felhasználói élményt, illetve erőforrás-megtakarítást tesz lehetővé a webserverek számára. A dinamikus tartalmak továbbra is webszervertől érkeznek. A webserverek fűrtözése esetén különböző algoritmusok alapján a fizikai gépek között terheléelosztást végez, illetve alkalmas SSL offloading megvalósítására.

A protokoll ellenőrzés révén kivédi a webservert esetleges rejtett sebezhetőségeinek, illetve a weboldal programozása során elkövetett hibák egy részét.

A WEBgw használható kliensek védelmére is. Ebben az esetben a statikus tartalmak elérésének gyorsításán felül vírusszűrő funkciókat is elláthat.

## QoS

Napjainkban a felhasználók egyre szélesebb körben vesznek igénybe a hálózaton keresztül elérhető olyan szolgáltatásokat, melyek adott sávszélességet vagy késleltetést igényelnek (pl. VoIP). Az ilyen jellegű szolgáltatások megfelelő működéséhez sok esetben prioritást kell felállítani a forgalmak között. Jellemzően nem megengedhető, hogy a VoIP-on folytatott beszélgetés szakadozzon, mert egy kolléga éppen adatokat tölt le egy távoli szerverről, amely a VoIP adatfolyamot oly mértékben késlelteti, hogy a beszélgetés ellehetetlenül.

Az esetek egy részében nem a rendelkezésre álló fizikai sávszélesség okozza az adatátviteli problémát, hanem a sávszélesség átgondolatlan felhasználása.

Az **Andrews Kft.** által használt QoS megoldás segítségével a fenti probléma elkerülhető, mert lehetőséget biztosít arra, hogy adott tulajdonságú adatfolyamot a többi elé lehessen helyezni, ezáltal biztosítva számára a minimális késleltetést. Többé nem kell attól tartani, hogy egy nagy állomány átvitele távoli szerverre megbénítja az egyéb hálózati forgalmakat, mert lehetőség nyílik adatfolyamonként a felhasználható sávszélesség maximalizálására, illetve minimálisan garantált sávszélesség biztosítására.

## IDS

Sok esetben csak akkor veszik észre az informatikai rendszer üzemeltetői, hogy támadás érte őket, mikor a rendszerbe már behatoltak, és nem kívánt változtatásokat hajtottak végre. Ebben az esetben nem marad más hátra, mint elemezni a behatolás mikéntjét, megerősíteni a rendszer gyenge pontját, és reménykedni, hogy nem jutottak értékes adatokhoz a támadók.

Az **Andrews Kft.** által használt IDS szolgáltatás képes a már folyamatban lévő támadásokat detektálni, riasztani az illetékest, aki már támadás folyamán megteheti a szükséges lépéseket a támadás kivédéséhez.

Az IDS folyamatosan figyeli a hálózati forgalmat, és az adatfolyamban támadásra utaló mintákat keres, így már azelőtt képes felderíteni a támadást, mielőtt még a rendszert kompromittálnák. A behatolásérzékelő naprakész adatbázissal rendelkezik, amely folyamatosan bővül az újabb támadások tipikus ismertetőjeleivel.



## Oktatás, képzés, technikai/ kereskedői bemutatók

**Az Andrews Kft. egyik fő tevékenysége az üzemeltetés, mely során szinte napi kapcsolatban áll az ügyfeivel. A közös projektek során számtalanszor hangzik el a kérdés: „és hol lehet mindezt megtanulni?”. Az első idők pár perces „oktatásai” az idők folyamán több napos tanfolyamokká nőttek ki magukat, melyek során egy-egy témát az adott feladathoz szükséges mélységben sajátítják el a résztvevők.**

Legfontosabb oktatási területek a hálózat- és programozásbiztonsággal, Linux, \*BSD és Solaris fejlesztéssel és üzemeltetéssel kapcsolatos témakörök.

A tanfolyamok kialakítása az ügyfelek igényeinek figyelembe vételével történt. A tanfolyamok nem kötött anyagúak, a meghirdetett tematika és időtartam tájékoztató jellegű, a konkrét tananyag a Megrendelővel történt előzetes egyeztetés (igény-és szintfelmérés) alapján kerül véglegesítésre.

A tanfolyamok díjazása függ a résztvevők számától, a tanfolyam helyszínétől és a szükséges infrastruktúra biztosításának módjától. Az oktatások jellemzően a Megrendelő telephelyén/oktatótermében kerül megvalósításra, de igény esetén az **Andrews Kft.** is biztosít minden szükséges infrastruktúrát.

A tanfolyamok üteme igazodik a Megrendelő igényeihez. Szükség esetén fél napos egységekben történik az oktatás, illetve az oktatások időpontjainak kezelése is rugalmas.

Egy napi oktatás 8x45 percből áll, ami általában 4x1.5 órára tagolódik. A legtöbb oktatás jelentős része gyakorlat, ami elősegíti az anyag jobb megértését és rögzülését. A tanfolyam után lehetőség biztosított további konzultációra is.

Az oktatók közül többen rendelkeznek a magas szintű műszaki ismeretek mellett tanári diplomával és több éves tanítási gyakorlattal is, illetve az évek során számos konferencián szerepeltek mint előadók.

Az **Andrews Kft.** ügyfelei oktatása mellett nagy hangsúlyt fektet partnerei és viszonteladói képzésére és sales támogatására is.

Tanfolyamaink (a teljes listát a <http://www.andrews.hu/trainings.hu.html> lapon található):

**TCP/IP szakértői tanfolyam**  
**VMware tanfolyam**  
**Linux Enterprise környezetben**  
**Központi felhasználó kezelése KERBEROS és LDAP segítségével**  
**Haladó hálózati adminisztrátor Linuxon**  
**Számítógépes biztonság alapjai**  
**Általános adminisztrátori ismeretek**  
**Hibakeresés Linuxon**

### TCP/IP szakértői tanfolyam

**Tanfolyam szintje:** haladó +++

**Időtartam:** 5 nap  
Teljesen disztribúciófüggetlen tanfolyam.

**A tanfolyam célja:** A tanfolyam résztvevői megismerik a TCP/IP protokollcsaládot teljes részletességgel (ami alatt a legtöbb esetben bit szintű ismertetést értünk). A TCP protokollal különösen részletesen foglalkozunk, a hallgató megismerheti az egyszerű felhasználók és rendszergazdák által nem látható, háttérben zajló folyamatokat. A hallgató a tanfolyam elvégzése után képes lesz a legösszetettebb TCP/IP kommunikációs problémák megtalálására, TCP/IP stack-ek működésének megértésére, programozási ismeretek birtokában esetleg implementálására is. A tanfolyamot csak erős TCP/IP alapokkal rendelkező hallgatóknak ajánljuk.

**Tematika vázlat:**

- ➔ TCP/IP általában
- ➔ Adatkapcsolati szint
- ➔ IP csomag szerkezete
- ➔ A routing alapjai, adatkapcsolati és hálózati réteg kapcsolata, az ARP protokoll
- ➔ ICMP protokoll
- ➔ IP routing, valamint az ICMP protokoll
- ➔ UDP protokoll
- ➔ Broadcast és multicast kommunikáció, multicast routing, IGMP



- TCP protokoll alapjai
- TCP kapcsolat felépítése és lezárása
- TCP interaktív adatátvitel
- TCP nagy tömegű adatátvitel
- TCP timeout és újrabadás
- A TCP protokoll teljesítményhangolása
- A TCP/IP protokollcsalád gyengeségei, hálózati támadások

## Linux Enterprise környezetben

**Tanfolyam szintje:** haladó

**Időtartam:** 5 nap  
Teljesen disztribúciófüggetlen tanfolyam.

**A tanfolyam célja:** A Linux operációs rendszer vállalati szintű felhasználáshoz szükséges képességeinek ismertetése. A tanfolyam keretében bemutatottak komplexitása nem teszi lehetővé az egyes képességek részletes ismertetését, ezért a tanfolyam keretében a képességek operátori szintű bemutatására szorítkozunk. Igény esetén adott témában szakértői tanfolyamokat, illetve konzultációkat szervezünk.

### Tematika vázlat:

- Linux alapú rendszerek teljesítményhangolása
- Linux kernel memóriakezelése
- Linux kernel hálózati alrendszerének teljesítményhangolása
- Diszk alrendszer, illetve állományrendszerek (filesystems) teljesítményhangolása
- Többprocesszoros rendszerek hangolása
- Magas rendelkezésre állás, hibatűrő rendszerek
- Naplózó állományrendszerek
- Hibatűrő disk alrendszerek kialakítása (RAID)
- Logikai partíciók megvalósítása (LVM)
- Monitoring rendszerek
- Nagios hálózati felügyeleti rendszer bemutatása, lehetőségei
- Terheléelosztás, megosztott erőforrások
- Hálózati erőforrások terheléelosztása (LVS)
- Magas rendelkezésre állású hálózati szolgáltatások (HA)
- Virtualizációs technológiák
- Virtualizáció elmélete, gyakorlati előnyei
- Elterjedt virtualizációs technológiák Linuxon: XEN – UML – VMware ESX server – KVM

## Haladó hálózati adminisztrátor Linuxon

**Tanfolyam szintje:** haladó

**Időtartam:** 5 nap  
Teljesen disztribúciófüggetlen tanfolyam.

**A tanfolyam célja:** A tanfolyam elvégzése után a hallgatók képesek lesznek Linux alapú rendszerek hálózati alrendszerének üzemeltetésére, biztonságos hálózati topológiák kialakítására valamint az üzemeltetett rendszerekkel kapcsolatban felmerülő hálózati hibák elemzésére, elhárítására. A tanfolyam magába foglalja a TCP/IP protokoll adminisztrátori szintű ismertetését.

A tanfolyam további célja a következő témakörök Linux alapú megvalósításának ismertetése:

- Titkosított magánhálózatok (Virtual Privat Network – VPN)
- Hálózati sávszélességmenedzsment alapjai
- Linux kernel hálózati útválasztó rendszere – Advanced Routing

### Tematika vázlat:

- Hálózati kommunikáció alapjai, TCP/IP hálózatok
- Linux hálózati alrendszer
- Hálózati szegmentáció, topológia tervezése
- Linux kernel csomagszűrő tűzfal alrendszere
- Titkosított magánhálózatok alapjai, linuxos megvalósítása gyakorlatban
- Hálózati sávszélességmenedzsment alapjai
- Advanced routing képességei, felhasználási lehetőségei a gyakorlatban

## Számítógépes biztonság alapjai

**Tanfolyam szintje:** kezdő

**Időtartam:** 5 nap  
Teljesen disztribúciófüggetlen tanfolyam.

**A tanfolyam célja:** A tanfolyam résztvevői megismerik korunk számítógéprendszereinek sebezhetőségeit, azok kihasználásának elvi lehetőségeit és a kihasználás elleni védekezés módjait. A tanfolyam részei a bevezető kriptológiai (titkosítással kapcsolatos) és a biztonságos fejlesztési alapismeretek is.

### Tematika vázlat:

- Bevezető, általános alapok
- Tipikus programozási hibák és kihasználásuk
- Helyi biztonság Unix rendszereken
- Linux rendszerek biztonsági kérdései
- A Linux kernel magas biztonságú kiegészítései
- Biztonságos Linux szerver telepítése
- Számítógépes hálózatok biztonsági kérdései (IP, TCP, UDP, ICMP)
- Tűzfalak típusai – csomagszűrő, állapotartó csomagszűrő, alkalmazásszűrő
- Védelmi terv, hálózati hiba demonstráció
- A Linux állapotartó csomagszűrője
- Kriptológia
- Biztonságos fejlesztés, audit – CC



## Hálózati kiszolgálók, szerverek

Az Andrews Kft. által üzemeltetett rendszerek lelkét a baseOS adja, amely a mai modern üzleti szolgáltatásokat kiszolgáló szoftverek széles skáláját tartalmazza. A baseOS Linux alapú, egyedi biztonsági igényekhez alakított speciális operációs környezet, melyben az ismeretlen sebezhetőségek ellen a rendszer speciális, biztonsági szempontokat előtérbe helyező felépítése nyújt védelmet. Minden szolgáltatás leválasztott biztonsági környezetben működik, így egy szolgáltatás kompromittálódása esetén az alaprendszerhez és a többi szolgáltatáshoz vezető úton még további, belső védelmi, sorompók állják az esetleges támadó útját. A baseOS részeit képező alkalmazásokat az Andrews Kft. munkatársai folyamatosan ellenőrzik, és a TCB rendszer segítségével napra készen tartják, minimalizálva az ismert sebezhetőségek adta kockázatot.

Az alábbi felsorolás csupán ízelítőként próbálja bemutatni a baseOS lehetőségeit, melyek a Linux rugalmasságának köszönhetően, szinte határtalanok. Speciális ügyféligény esetén, szinte tetszőleges kiszolgáló megvalósítása lehetséges a baseOS-re építkezve (pl Linux alapú Lotus Notes kiszolgáló, egyedi fejlesztések eredményeként létrejött Linux alapú alkalmazások).

Amennyiben fokozott üzem és informatikai biztonságú, Linux alapú hálózati kiszolgálóra van szüksége, válassza az **Andrews Kft.** baseOS-ét!

### HA

Az **Andrews Kft.** által szállított rendszerek képesek szinte minden szolgáltatást fűrtözve futtatni. Az egyik tag kiesése esetén a másik azonnal átveszi szolgáltatásokat. Ezzel extrém magas rendelkezésre állást lehet megvalósítani és nagymértékben

csökkenteni lehet a tervszerű leállásokból, karbantartásokból adódó kieséseket is.

### Webkiszolgálás

Az üzleti életben a jelenleg legelterjedtebb webkiszolgáló az Apache. Népszerűségét a jó skálázhatóságának, a nagy fokú modularitásának és legendás megbízhatóságának köszönheti. Az egyszerű személyes weboldalak kiszolgálására ugyanolyan alkalmas, mint az óriási forgalmat lebonyolító hírporálok kezelésére, illetve a nagyvállalati belső web alapú rendszerek futtatására.

Az Apache sok keretrendszert, programozási nyelvet támogat ezek közül a legnépszerűbbeket az **Andrews Kft.** szerverei is alaptól támogatják. Az üzleti életben már régóta jelen levő, sokszor bizonyított JAVA alkalmazásszerverek közül az Apache Tomcat elérhető és a weben nagyon elterjedt, a nagyvállalati megoldásokban is egyre gyakrabban alkalmazott PHP és Perl is elérhető.

A webkiszolgáló képes a már meglévő vállalati Oracle, MSSQL, PostgreSQL vagy MySQL adatbázis szerverhez csatlakozni illetve lehetőség van helyi PostgreSQL vagy MySQL szerver telepítésére is.

### Adatbázis kezelés

Az baseOS ideális futási környezetet biztosít adatbázis kezelő kiszolgálók használatához, melyek közül az alábbiak érhetőek el:

Oracle, az adatbázis kezelő piac kvázi szabványa, nagy teljesítményű, robusztus adatbázis szerver.

PostgreSQL egy legendásan stabil, számos szolgáltatással rendelkező ingyenes adatbázis kiszolgáló. A PostgreSQL elérhető számos Unix típusú operációs rendszeren, MVCC (Multi Version Concurrency Control, több egyidejű verzió vezérlése) nevű társtratégiát alkalmaz – csak úgy mint jó néhány kereskedelmi termék, ennek köszönhetően alkalmas nagyméretű rendszerek kiszolgálására is. Többek között támogatja a triggereket, tranzakciókat, replikációt. Nagy méretű, adatbázisok, illetve összetett adatbázis logika esetén ajánlott.

Mysql (a PostgreSQL-hez képest) egy szerényebb tudású adatbázis kezelő. Egyik leggyakrabban használt, adatbázis keze-



lő alkalmazás, a webszolgáltatások körében. Népszerűségét gyorsaságának illetve széleskörű támogatottságának köszönheti. Elérhető számos Unix típusú operációs rendszeren, illetve Windows platformon.

### Levelező kiszolgáló

Napjainkban az elektronikus levelezés, a leggyakrabban használt szolgáltatás az Interneten. Manapság a mindennapi üzletmenethez nélkülözhetetlen, a gördülékeny kommunikáció elengedhetetlen része az e-mail. Azonban előnyei ellenére rejt magában veszélyeket is, a felhasználónak naponta meg kell küzdeni a kéretlen levelekkel, a mellékletben érkező vírusok, és egyéb kártevők veszélyeztetik az informatikai rendszer integritását.

Az **Andrews Kft.** által szállított e-mail rendszer, mely nyílt forrású elemekre épül, ezen problémákra is nyújt megoldást. Az általuk szállított rendszer képes önállóan is megfelelni a levelezéssel szemben támasztott követelményeknek, de a már meglévő infrastruktúrába is könnyen beilleszthető. Integrált **SPAM**-szűrője lévén a megszabadítja a felhasználókat, a kéretlen

levelektől, a beépített vírusszűrő hatékonyan akadályozza meg a kártevők bejutását a védett hálózatba.

### Fájlszerverek

A virtualizáció első lépcsőjét jelentették a hálózati tárolók megjelenése. Használatukkal, egy közös helyre összpontosították a háttértár erőforrásokat, ilyen módon maximalizálva ezen háttértárak kihasználhatóságát és megkönnyítve felügyeletüket. Az **Andrews Kft.** baseOS kiváló alapot biztosít, Linux alapú, fájlserver megvalósítására.

Támogatott hálózati protokollok: FTP, HTTP, WEBDAV, CIFS, SMBFS, SSHFS, NFS, iSCSI

Támogatott RAID technológiák: RAID0, RAID1, RAID4, RAID5, RAID6, RAID0+1

A Linux kernel Logical Volume Manager által biztosított képességek: – snapshot (pillanatfelvétel) a használt tárterületről, kiesésmentes vagy minimális kieséssel járó mentési megoldások megvalósításához – rugalmas háttértár kezelés, leállítás-mentes bővíthetőség, átméretezhetőség képessége



## Üzemeltetés, karbantartás

**Egy informatikai rendszer életciklusának üzleti szempontból legfontosabb és időbeli lefolyását tekintve leghosszabb része a működési, karbantartási szakasz.**

A karbantartás és üzemeltetés megvalósításának alapvető problémái, hogy

- a magára hagyott rendszer az idő múlásával arányosan egyre több ismert sérülékenységet és hibát tartalmazhat több rendszer frissítése időigényes, nehézkes az üzemeltetői csapat fenntartása költséges, illetve bizonyos számú rendszer alatt nem hatékony egy belső csapat fenntartása, folyamatos képzése
- egy üzemeltetési infrastruktúra precíz kialakításának hiánya esetén a hibák detektálása, jelzése, felderítése nehézkes és időigényes
- A működési, karbantartási szakasz két sarkalatos pontja a rendszer karbantartása, ellenőrzött frissítése
- folyamatos monitorozása és a fellépő hibák elhárítása

Az **Andrews Kft.** a fenti feladatokat saját fejlesztésű menedzsment, monitorozó és elemző modulok segítségével látja el, melyek egyenként, illetve kombinálva állnak az ügyfelek rendelkezésére. Szakértői csapata tapasztalatával és naprakészen tartott tudásával kínál megoldást a folyamatosan változó környezet biztonsági és üzemeltetési problémáira. Kiemelt figyelmet szentel a különböző informatikai biztonság terén megjelenő publikációk, kutatások és biztonsági levelezési listák olvasásának, hogy a cég által karbantartott és üzemeltetett rendszerek biztonsága folyamatosan a legmagasabb szinten maradjon.

### Konfiguráció menedzsment és üzemeltetés

#### Tömeges szerver üzemeltetés és ellenőrzés (TCB)

A TCB rendszer hatékony eszközt biztosít jelentős mennyiségű UNIX/Linux szerver központosított – mégis rugalmas – te-

lepítésére, üzemeltetésére, frissítésére, konfigurációs állományainak központi karbantartására. Az üzemeltetett rendszerek komponensei virtuális csomagokra bontva a központi rendszeren tárolt etalon adatbázisba kerülnek. Az üzemeltetett rendszerek tetszőleges szempontok alapján logikai csoportokba szervezhetők és egységként kezelhetők. (pl.: feladat vagy operációs rendszer szerint).

Az üzemeltetéssel és frissítéssel kapcsolatos feladatokat a központi etalon állományokon kell csak elvégezni – azaz egy helyen, és nem minden üzemeltetett rendszeren külön-külön. Az így előidézett változások a TCB rendszer segítségével gyorsan és biztonságosan életbe léptethetőek – visszavonhatóak – valamennyi üzemeltetett rendszeren.

Hatékony mentési és katasztrófa elhárítási képességeinek köszönhetően az üzemeltetett rendszer teljes megsemmisülése esetén is rövid időn belül visszaállítható a produktív környezet.

#### DHCP és DNS konfiguráció (DHCPMan)

A DHCPMan kiterjedt hálózatok DNS és DHCP szervereinek adminisztrációját egyszerűsíti le. Központi konfigurációs állományban tárolt, a teljes hálózat felépítését leíró adatok, a hálózatban található gépek adatait tartalmazó adatbázisa és előre elkészített template-ek alapján képes kigenerálni a szükséges DHCP és DNS szerverek konfigurációs állományait (beleértve a zóna fájlokat is). Használatával kiküszöbölhető a DNS és DHCP szerverek adatainak inkonzisztenciája és egy bonyolult hálózat komplett átalakítása (DHCP és DNS szinten) a több napos munka helyett néhány óra alatt megvalósítható.

### Felügyelet

#### Monitoring

Üzleti szempontból kritikus szolgáltatások üzemeltetése, folyamatos felügyeletet megvalósító, monitorozó rendszerek használata nélkül elképzelhetetlen. Az **Andrews Kft.** által üzemeltetett rendszerek felügyeletét a Nagios hálózati monitorozó rendszer valamint a saját fejlesztésű CTS kiegészítő valósítja meg. Az így kialakított monitorozó rendszer minden, a folyamatos üzletme-



nethez szükséges erőforrást és szolgáltatást mélyrehatóan ellenőriz és felügyel UNIX/Linux és Windows operációs rendszert futtató gépeken illetve egyéb hálózati eszközökön.

A monitorozó rendszer segítségével folyamatosan (és visszamenőleg is) nyomon követhető a rendszer erőforrásainak kihasználtsága, a forgalmi/hálózati adatok. A rendszerek elemeinek állapotában bekövetkező változásokhoz figyelmeztetések rendelhetők, így az üzemeltetés során előforduló problémák jelentős része még a kialakulásuk kezdetén felfedezhető és kezelhető.

### Logelemzés

Az emberi erőforráson alapuló logfeldolgozás több okból nehézkes és gyakran kivitelezhetetlen. Az egyes alrendszerek tevékenysége során keletkező naplóbejegyzések összessége a legtöbb esetben igen nagy mennyiségű és gyakran már egyetlen gép esetén is lehetetlenné teszi az emberi feldolgozást. Az **Andrews Kft.** saját fejlesztésű logelemző rendszere egy moduláris felépítésű, többszintű, erőforrás kímélő logfeldolgozó, amely syslog formátumot kezel (felépítésének köszönhetően könnyedén illeszthető más szöveges logformátumokhoz is), adaptív mintaadatbázissal és webes megjelenítő felülettel rendelkezik. Az eszköz remekül alkalmas a rendszerekben bekövetkezett események alapján statisztikák készítésre, különböző események közötti korrelációk felismerésére és megadott eseményekhez rendelt döntések vagy határértékek elérése esetén riasztások küldésére.

### Riasztás

Kritikus rendszerek felügyelete és üzemeltetése során rendkívül fontos, hogy minden lényeges eseményről rövid időn belül értesüljenek a rendszert karbantartó személyek. A jelenlegi gyakorlat szerint ezek az értesítések általában emailben kerülnek továbbításra, ami komoly kockázatot hordoz magában, ugyanis számos feltételnek kell teljesülnie ahhoz, hogy az email alapú értesítés időben érkezzon, és valóban meg is érkezzon a megfelelő személyekhez.

Néhány ezen feltételek közül:

- Hálózati kapcsolatnak kell lennie a küldő és a címzett rendszerek között. Sok esetben ezen kapcsolat hiánya az a kritikus esemény, amiről értesítést kellene küldeni.
- Az email továbbító rendszereknek (mail szervereknek) tudniuk kell fogadni és továbbítani, elfogadható időn belül a riasztásokat. Amennyiben a továbbítási lánc valamely eleme nem működik megfelelően, vagy csak jelentős késleltetéssel képes továbbítani a riasztásokat úgy szintén késve értesül a problémáról a rendszer üzemeltetője.
- Amennyiben a hálózati kapcsolat működik és a riasztást tartalmazó email is megérkezik, akkor azt valakinek el kell azt olvasnia, lehetőség szerint bármikor és bárhol is van a rendszerek felügyeletéért felelős személy(zet). A nap 24 órájában folyamatos adminisztrátori felügyelet biztosítása csak igen magas költségekkel valósítható meg. Magyarországon, a nagyvállalati illetve pénzügyi és egyéb kritikus szektorokat leszámítva, ilyen felügyeleti rendszer felállítása és üzemeltetése cégen belül nem valósítható meg költség hatékony módon.

Amennyiben ezen feltételek valamelyike nem teljesül, abban az esetben a kritikus hiba elhárítása nem kezdődhet meg időben, mivel a felügyeletért felelős személynek nem is lesz tudomása a hiba létéről.

Az **Andrews Kft.** által kínált SMSGW megoldást nyújt ezen problémákra, valamint további szolgáltatásokat képes biztosítani.

A megoldás lényege, hogy a kritikus riasztás közvetlenül GSM hálózaton, GSM telefon vagy modem segítségével kerül továbbításra, ezáltal az internetes infrastruktúrától független kommunikációs csatornát biztosít. Az SMSGW közvetlenül a felügyelő eszközök közelében kerül elhelyezése, így annak az informatikai hálózattól való függése minimálisra csökkenthető.

Rugalmas beállíthatóságának és egyszerű kapcsolódási felületének köszönhetően könnyen illeszthető meglévő felügyeleti rendszerekhez, ezáltal kiegészítve azok működését.



## Virtualizáció

**Az Andrews Kft. 2006 óta tevékenykedik VMware Enterprise partnereként. Az évek során számos integrációs projektben és rendszerauditban vett részt tanácsadóként, illetve kivitelezőként, melynek köszönhetően jelentős és egyedi tapasztalatot, tudást gyűjtött össze a VMware különböző termékcsaládjával kapcsolatban.**

A VMware ESX szerver terméke és a hozzá kapcsolódó környezet évek óta stabilan a legjobb teljesítményű, megbízható, enterprise környezetbe leginkább illeszkedő rendszer a virtualizációs megoldások mezőnyében.

### Virtualizáció járulékos előnyei:

- Csökkenő hardverszám
- karbantartási költségek csökkenése
- csökkenő villamosenergia-fogyasztás
- kisebb hűtési igény
- kisebb helyigény (csökkenő bérleti költségek)
- Egységes virtuális hardverfelület
- Hatékony erőforrás-felhasználás biztosítása
- Rugalmas skálázhatóság
- Kisebbs humán erőforrás igény
- Magasabb rendelkezésre állás

Az **Andrews Kft.** hisz abban, hogy még a legmegbízhatóbb virtuális környezet sem hagyható magára, folyamatos üzemeltetést, monitorozást, frissítést igényel, hogy hosszú távon képes legyen az elvárt teljesítményt és megbízhatóságot nyújtani.

A cég az integrációk során arra törekszik, hogy a lehetőségekhez mérten, a tőle már megszokott hálózati biztonsági szintet nyújtsa virtuális környezetben is.

A VMware termékének megfelelő csomagjai lehetőséget biztosítanak arra, hogy a közép- és nagyvállalati szféra mellett a kisvállalatok is ki tudják használni a virtualizációban rejlő potenciális lehetőségeket.

### Szolgáltatások:

- Technikai/kereskedői bemutatók [DEMO] – Döntéselőkészítés támogatása
- Igény-, rendszerfelmérés [PRESALES] – Ajánlat/rendszerterv kidolgozása
- Üzembehelyezés [INTEGRATION] – Igényeknek megfelelő rendszer megvalósítása
- Oktatás, képzése [EDUCATION] – Egyedi oktatások, üzemeltetői képzések
- Üzemeltetés, karbantartás [SUPPORT] – Technikai segítségnyújtás, támogatás (7x24)
- Minőségbiztosítás [QA] – Frissítések ellenőrzése tesztkörnyezetben
- Felügyelet, ellenőrzés [MONITORING] – Virtuális környezet folyamatos felügyelete
- Felülvizsgálat [AUDIT] – Meglevő rendszerek auditálása, tanácsadás
- Technikai/kereskedői bemutatók [DEMO]

Az **Andrews Kft.** vállalja igény szerinti technikai, kereskedői vagy vegyes bemutatók tartását mind leendő, mind meglévő ügyfeleinek, illetve mindenki számára, akinek felkeltette érdeklődését a VMware virtualizációs világa. A jelenleg legnépszerűbb bemutatók: VI, VIEW, vSphere forecast.

### Igény-, rendszerfelmérés [PRESALES]

Az **Andrews Kft.** részletesen kidolgozott igényfelmérést végez annak érdekében, hogy Ügyfelei pontosan arra a megoldásra kapjanak ajánlatot, amelyre valóban szükségük van és amit meg szeretnének valósítani. A cég mérnökei a felmérés során feltárják a valós igényeket, segítenek megtalálni a legmegfelelőbb megoldást, és annak megfelelően készítik el ajánlatukat. Csak a jól tervezett rendszer lehet a megfelelő alap az induláshoz.

### Üzembehelyezés [INTEGRATION]

Az igényfelmérés során kialakult képből rendszerterv készül. A terv alapján – pontos időzítésekkel – kezdődik meg az integráció, a folyamat közben felmerülő és megoldandó igények szem előtt tartásával úgy, hogy a rendszer kiépítése a lehető legkevesebb üzemkiesést okozza. Amennyiben az oktatással egybekötött üzembehelyezést választja a Megrendelő, úgy a folyamat



végén nem fekete dobozt kap, hanem egy általa megismert és hasznosnak ítélt, átlátható és testre szabott rendszert.

### **Oktatás, képzések [EDUCATION]**

Az **Andrews Kft.** egyedi kidolgozású és kipróbált tematikájú oktatásokat szervez VI, VIEW és storage témákban. Haladó szintű, gyakorlati VI oktatást is biztosít igény szerint, mely során a hibakeresés és hibakezelés, helyreállítás témákban mélyülhetnek el alaposabban az arra vállalkozók.

### **Üzemeltetés, karbantartás [SUPPORT]**

Az **Andrews Kft.** üzemeltetői csapata a hét minden napján 24 órában áll rendelkezésre. Az általuk üzembehelyezett rendszereket folyamatosan felügyelik, az általuk előzetesen kipróbált patchekkel frissítik, az esetleges problémákat rövid reagálási idővel, akár azonnali beavatkozással kezelik.

### **Minőségbiztosítás [QA]**

A cég az ügyfelei számára fenntartott tesztrendszereiken folyamatosan teszteli a kiadott gyári frissítéseket, elemezi a teszt során felmerülő változásokat és hibákat, és csak abban az esetben végezi el a frissítést, ha azt biztonságosnak ítéli. Az **Andrews Kft.** támogatásával nem érhetik kellemetlen meglepetések.

### **Felügyelet, ellenőrzés [MONITORING]**

A virtuális futtatókörnyezet monitorozása éppen olyan fontos, mint a rajta futó rendszerek felügyelete. Az **Andrews Kft.** által fejlesztett ESX monitorozó kiegészítés segítségével a cég mérnökei olyan rendellenességeket is előre észlelnek, amelyekre még nem jelentek meg gyártói figyelmeztetések, és így időben meggátolható a hiba bekövetkezése, de az információ gyors beavatkozást tud biztosítani egyszerű tárhely probléma és/vagy memória szivárgás okozta memóriafogyás esetén is.

### **Felülvizsgálat [AUDIT]**

Felülvizsgálat során az **Andrews Kft.** a nem karbantartott, korszerűtlen virtuális környezeteket feltérképezi, javaslatot tesz a feltárt problémák javításaira, azok ütemezésére, további felkérésre a környezet rendbetételét is vállalja. Azon virtuális környezetek, amelyeket nem felügyelnek, idővel törvényszerűen ebbe a helyzetbe kerülnek, így javasolt minél előbb az üzemeltetés mellett dönteni. Minél rövidebb ideig volt magára hagyva egy rendszer, annál kisebb feladat az aktualizálása, korszerűvé tétele. Az audit során nagy figyelmet szentel a biztonságos kialakítás ellenőrzésére, mind hálózati, mind szoftver oldalon.