





# IT biztonság

## 2020/2021 tanév ősz

2020.11.09. ELTE IT Biztonság Speci 1

1



# Bemutakozás

**Giesz István**

- okl. Gépészmérnök, okl. Rendszerszervező, Információbiztonsági menedzser, ISO27k1IA&LA
- KÖFÉM/ALCOA, BUSZESZ, HUNGRANA, Csemege Julius-Meini, SPAR, TESCO - IT vezető/ügyvezető
- GIRO Zrt. - vezérigazgató helyettes
- Progradat Kft. - ügyvezető

2020.11.09. ELTE IT Biztonság Speci 2

2

## Agenda

- Információbiztonsági incidensek kezelése
- Működésfolytonosság biztosításának információbiztonsági vonatkozásai
- Naplózás és megfigyelés

2020.11.09.

ELTE IT Biztonság Speci

3

3

## Szabványok vs. Tematika fejezetek

Tematika	ISO/IEC 27001	NIST 800-53r4	41/2015 BM.
Naplózás és megfigyelés	A12.4	AU - Audit and Accountability	3.3.12. - Naplózás és elszámoltathatóság
Információbiztonsági incidensek kezelése	A16	IR - Incident Response	3.1.5. - A biztonsági események kezelése
Működésfolytonosság biztosításának információbiztonsági vonatkozásai	A17	CP - Contingency Planning	3.1.4. - Üzletmenet (üzymenet) folytonosság tervezése

2020.11.09.

ELTE IT Biztonság Speci

4

4

## Esemény

**Esemény<sup>27k1</sup>:** Valamilyen megfigyelhető változás egy információs rendszerben.

- Egy eseménynek lehet egy vagy több előfordulása, és több oka is lehet.
- Egy esemény lehet az is, hogy ha valami nem történik.

Információbiztonsági esemény<sup>27k1</sup>: olyan **esemény**, amely az információbiztonsági szabályok esetleges megsértését vagy a meglévő kontrollok hiányosságát, vagy egy korábban még ismeretlen helyzetet jelent, és amely biztonsági szempontból lényeges.

Információbiztonsági incidens<sup>FISMA</sup>: olyan **esemény**, amely törvényes felhatalmazás nélkül ténylegesen vagy közvetlenül veszélyezteti az információk vagy információs rendszerek titkosságát, integritását vagy elérhetőségét; vagy törvények, biztonsági irányelvek, biztonsági eljárások vagy elfogadható felhasználási irányelvek megsértésének vagy azok közvetlen fenyegetésének minősül.

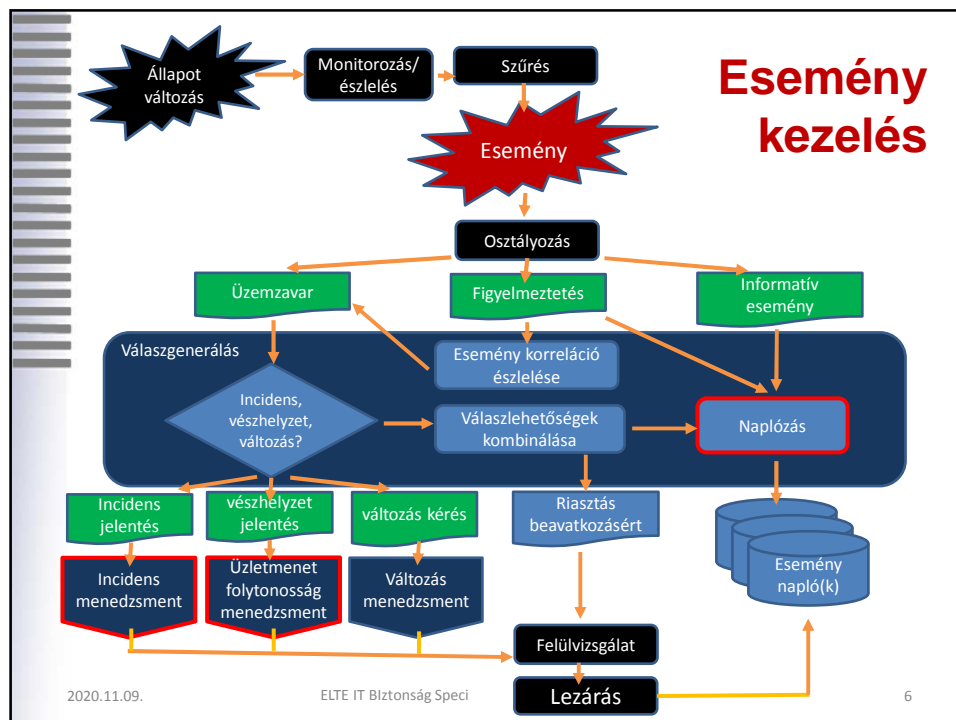
FISMA - Federal Information Security Modernization Act

2020.11.09.

ELTE IT Biztonság Speci

5

5



2020.11.09.

ELTE IT Biztonság Speci

6

6

## Fenyegetés

Fenyegetés: egy nem kívánt **esemény** lehetséges oka, amely kárt okozhat egy rendszerben vagy szervezetben.

Fizikai jellegű fenyegetések: az infrastruktúra fizikai elemeit és/vagy az embereket veszélyeztető, szándékos vagy véletlenszerű fizikai hatások, és/vagy elégtelenségekből adódó hibák.

Informatikai jellegű fenyegetés: lehet az infrastruktúra fizikai elemeit és/vagy az embereket veszélyeztető, szándékos vagy véletlenszerű, műszaki eszközök és/vagy módszerek segítségével érvényesülő káros hatások.

Emberi-szervezeti fenyegetések: szándékosak (szabotázs, vandalizmus, hacker-támadás stb.) vagy véletlenszerűek (pl. járvány, tömegdemonstráció stb.) lehetnek, esetleg adódhatnak a szervezeti elégtelenségekből (pl. létszámhiány, alul képzés, stb.)

2020.11.09.

ELTE IT Biztonság Speci

7

7

## Definíció

Információbiztonsági esemény típusok		
Incidens	Vészhelyzet, krízis	Katasztrófa
Emberi-szervezeti fenyegetések -> szándékos hacker-támadás	<ul style="list-style-type: none"> <li>Fizikai jellegű fenyegetések</li> <li>Informatikai jellegű fenyegetés</li> <li>Emberi-szervezeti fenyegetések</li> </ul>	Fizikai jellegű fenyegetések -> az elsődleges működési központ használhatatlanná válása

2020.11.09.

ELTE IT Biztonság Speci

8

8

## Információbiztonsági incidensek kezelése

2020.11.09.

ELTE IT Biztonság Speci

9

9

## Fenyegetések (emberi-szervezeti) -> INCIDENSEK

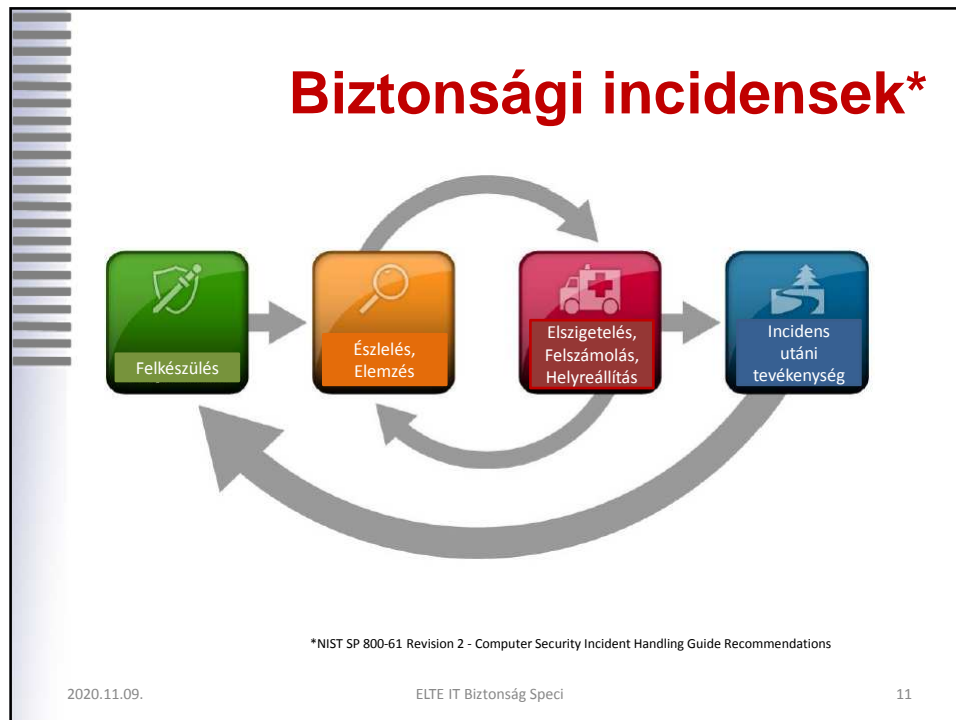
Fenyegetés formák	Motiváció	Tevékenység -> INCIDENS
hacker, cracker	kihívás, ego, lázadás	hackelés, social engineering, behatolás, jogosulatlan hozzáférés
számítógépes bűnöző	információmeg semmisítése, illegális információközlés, pénzszerzés, jogosulatlan adat megváltoztatás	rendszerbehatolás, spoofing, megvesztegetés, hacker technikák
terroristák	megsemmisítés, kihasználás, bosszú, rémhírterjesztés	rendszer támadás, DDOS, rendszer penetráció, rendszer hamisítás, Információs háború
ipari kémek (vállalatok, külföldi kormányzatok, más Kormányzati érdekeltségek)	gazdasági előnyök szerzése, versenyelőnyök, hírszerzés	információ lopás, social engineering, személyes adatok felhasználása, jogosulatlan rendszer hozzáférések (bizalmasadatok, technológiai adatok, stb.)
belső személyek	kíváncsiság, ego, információ szerzés, pénzszerzés, bosszú, hibák	munkavállaló megfenyegetése, rossz hír terjesztése, számítógépes csalás, információlopás, megszakítás, meghamisított adatok, rendszer sabotálás, stb.

2020.11.09.

ELTE IT Biztonság Speci

10

10



11

## Kommunikáció, felszerelés

- kontakt információk
- incidens jelentési mechanizmus
- jegykezelő, munkafolyamat támogató rendszer
- okostelefon
- titkosító szoftver (védett kommunikációhoz)
- vészhelyzeti helyszín
- biztonságos tároló felszerelés

2020.11.09. ELTE IT Biztonság Speci 12

12

## Incidens elemző hardver és szoftver eszközök

- **Digitális elemző munkaállomások** és / vagy biztonsági mentési eszközök lemezképek létrehozására, naplófájlok megőrzésére és egyéb releváns eseményadatok mentésére
- **Laptopok** olyan tevékenységekhez, mint például az adatok elemzése, a csomagok szippantása és a jelentések írása
- **Tartalék munkaállomások, kiszolgálók és hálózati berendezések, vagy ezek virtualizált megfelelőik**, amelyek sokféle célra felhasználhatók, például biztonsági másolatok helyreállítására és kártékony programok kipróbálására
- **Üres cserélhető adathordozó**
- **Hordozható nyomtató** a naplófájlok és más bizonyítékok másolatának kinyomtatásához nem hálózati rendszerekről
- **Packet snifferek és protokollelemzők** a hálózati forgalom rögzítésére és elemzésére
- **Digitális elemző szoftver** a lemezképek elemzéséhez
- **Cserélhető adathordozó** a programok megbízható verzióival, amelyek felhasználhatók bizonyítékok gyűjtésére a rendszerekből
- **Bizonyíték gyűjtő eszközök** beleértve az ipari laptopokat, digitális fényképezőgépeket, hangrögzítőket, bizonyítéktároló táskákat és címkéket, valamint bizonyítékszalagot, hogy megőrizték a bizonyítékokat a lehetséges jogi lépésekhez

2020.11.09.

ELTE IT Biztonság Speci

13

13

## Incidens analízáló erőforrások

- **Port-lista**, beleértve az általánosan használt portokat
- **Dokumentáció** operációs rendszerekhez, alkalmazásokhoz, protokollokhoz, IDS és víruskereső termékekhez
- **Hálózati topológiák és a kritikus eszközök listája**, például adatbázis kiszolgálók
- Hálózatok, rendszerek és alkalmazások **alap konfigurációi**
- A kritikus fájlok **hash lenyomatai** az események elemzésének, ellenőrzésének és felszámolásának felgyorsítása érdekében

2020.11.09.

ELTE IT Biztonság Speci

14

14

## Incidens kezelő szoftver eszközök

- **Hozzáférés az image-ekhez** az operációs rendszerek és az alkalmazások újra telepítése és helyreállítása céljából

2020.11.09.

ELTE IT Biztonság Speci

15

15

## Incidens megelőző tevékenységek

- Kockázat elemzés (pl. annak meghatározása, hogy milyen fenyegetés és sebezhetőségek kombinációk jelennek meg)
- Host-ok hardening-je, napra kész patch-elés, stb.
- Hálózat biztonság - minden olyan tevékenységet megtagadása, amely kifejezetten nem engedélyezett
- Rosszindulatú szoftverek elleni védelem
- Felhasználói tudatosság fejlesztése, képzés

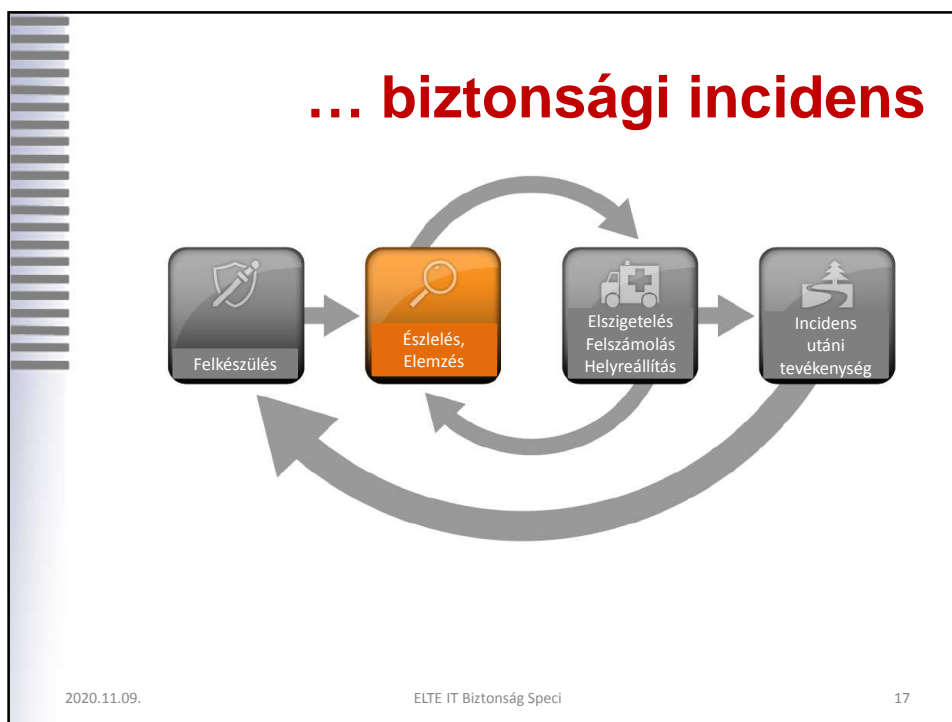
2020.11.09.

ELTE IT Biztonság Speci

16

16





17

## Támadási formák

- **Külső, mobil médiák:** ezen eszközről végrehajtott támadás
- **Felőrlés:** olyan támadás, amely durva erőszakos módszereket alkalmaz a rendszerek, hálózatok vagy szolgáltatások megsértésére, lebontására vagy megsemmisítésére.
- **Web:** webhelyről vagy webalapú alkalmazásból végrehajtott támadás
- **E-mail:** E-mailben vagy mellékletben végrehajtott támadás
- **Mások személyi adataival való visszaélés:** jóindulatú dolog rosszindulatúval való helyettesítése (pl. spoofinf, Man is the middle támadás, stb.)
- **Helytelen használat:** minden olyan esemény, amely a szervezet elfogadható használati irányelveinek meghatalmazott felhasználó általi megsértéséből ered
- **Berendezések elvesztése vagy ellopása**

2020.11.09. ELTE IT Biztonság Speci 18

18

## Incidens jelei

- Az incidenseket **sokféle eszközzel** lehet felismerni, változó részletességgel és megbízhatósággal.
- Az incidensek lehetséges **jeleinek mennyisége / mértéke jellemzően magas** (pl. nem normális, ha egy szervezet naponta több ezer vagy akár millió behatolást érzékelő riasztást kap).
- **Alapos, speciális technikai ismeretekre** és kiterjedt tapasztalatokra van szükség az eseményekkel kapcsolatos adatok megfelelő és hatékony elemzéséhez.
- Az esemény jelei a következő két kategóriába sorolhatók: **jelzők** és **indikátorok**.
  - **jelző:** azt mutatja, hogy a jövőben esemény történhet
  - **indikátor:** annak a jele, hogy incidens megtörtént vagy folyamatban van

2020.11.09.

ELTE IT Biztonság Speci

19

19

## Jelző és indikátor eszközök

Eszköz	Leírás
<b>Riasztók</b>	
IDPS-ek	Az IDPS-ek azonosítják a gyanús eseményeket és rögzítik a vonatkozó adatokat, beleértve a támadás észlelésének dátumát és időpontját, a támadás típusát, a forrás és a cél IP-címét, valamint a felhasználó nevet (ha alkalmazható és ismert).
SIEM-ek	A Biztonsági Információs és Esemény Kezelő (SIEM) termékek hasonlóak az IDPS-termékekhez, de riasztásokat generálnak a naplódatok elemzése alapján.
Antivirus és antispam SW-k	A víruskereső szoftver felismeri a rosszindulatú programok különböző formáit, riasztásokat generál, és megakadályozza, hogy a rosszindulatú programok megfertőzzék a host-okat.
Fájl integritást ellenőrző SW-k	A fájlok integritását ellenőrző szoftver képes észlelni az incidensek során a fontos fájlokban végrehajtott változásokat.
<b>Logok</b>	
Operációs rendszerek, szolgáltatások és alkalmazás logok	Az operációs rendszerek, szolgáltatások és alkalmazások naplói (különösen az audittal kapcsolatos adatok) gyakran nagy értéket jelentenek egy esemény bekövetkezésekor, például rögzítik, hogy mely fiókokhoz jutottak és milyen műveleteket hajtottak végre.
Hálózati eszközök logjai	A hálózati eszközökről, például a tűzfalakról és az útválasztókról érkező naplók általában nem az elsődleges forrásai a jelzőknek vagy az indikátoroknak.
Hálózati forgalom	A hálózati forgalom egy adott hálózati szegmensben, amely a host-ok között zajlik.

2020.11.09.

ELTE IT Biztonság Speci

20

20

## Jelző és indikátor eszközök

Eszköz	Leírás
Publikusan elérhető információk	
Információk az új sebezhetőségekről és kihasználhatóságáról	<a href="https://www.cert.hu">https://www.cert.hu</a> <a href="https://nki.gov.hu">https://nki.gov.hu</a> <a href="http://www.cert.org/csirts">www.cert.org/csirts</a> <a href="https://www.enisa.europa.eu/topics/csirt-cert-services">https://www.enisa.europa.eu/topics/csirt-cert-services</a> <a href="http://www.first.org/library">www.first.org/library</a> <a href="https://www.trusted-introducer.org">https://www.trusted-introducer.org</a>
Személyek	
Belső személyek	A felhasználók, a rendszergazdák, a biztonsági személyzet és mások a szervezetben belül jelenthetik az incidensek jeleit. Fontos minden ilyen jelentést érvényesíteni.
Személyek más szervezeteknél	Komolyan kell venni a külsőleg bekövetkezett események jelentését.

2020.11.09.

ELTE IT Biztonság Speci

21

21

## Incidens elemzés

- **Hálózati és rendszer profilok:** a profilalkotás és eltárolás az esetleges tevékenység jellemzőinek minősítését teszi lehetővé, hogy a változások könnyebben azonosíthatók legyenek.
- **Normál viselkedés megértése:** az incidens csoport tagjainak tanulmányozniuk kell a hálózatokat, rendszereket és alkalmazásokat, hogy megértsék, mi a szokásos viselkedésük, hogy a rendellenes magatartást könnyebben fel lehessen ismerni.
- **Napló megőrzés szabályozása:** az eseményekkel kapcsolatos információkat több helyen rögzíthetik, például tűzfal, IDPS és alkalmazásnaplók. A régebbi naplóbejegyzések a felderítést segítik a régebbi azonos vagy hasonló támadások korábbi példáit mutatva.
- **Esemény korreláció végzése:** az incidens bizonyítéka több naplóban rögzítődik, amelyek mindegyike különböző típusú adatokat tartalmaz - a tűzfalnaplóban lehet a forrás IP-cím, amelyet használtak, míg az alkalmazás naplóban felhasználónév szerepelhet.
- **Az összes host órájának szinkronban tartása**

2020.11.09.

ELTE IT Biztonság Speci

22

22

## Incidens elemzés

- **Információs tudásbázis karbantartása és használata**
- **Internetes kereső motorok használata:** az internetes kereső motorok segíthetnek az elemzőknek, hogy információkat találjanak a szokatlan tevékenységről.
- **Packet Sniffer alkalmazás futtatása további adatok gyűjtésére:** előfordulhat, hogy nincs elégséges részlet ahhoz, hogy a megértsük, hogy mi is történik. Ha egy hálózaton keresztül történik incidens, akkor a szükséges adatok gyűjtésének leggyorsabb módja az lehet, ha ilyen Packet Sniffer-t (WireShark) használunk a hálózati forgalom rögzítéséhez.
- **Adatok szűrése:** egyszerűen nincs elég idő az összes adat/jelzés áttekintésére és elemzésére.
- **Segítség kérés másoktól:** esetenként a csapat nem tudja meghatározni az esemény teljes okát és jellegét (CERT-ek!!)

2020.11.09.

ELTE IT Biztonság Speci

23

23

## Priorizálás

- **Incidens funkcionális hatása:** ezek a támadások befolyásolják a rendszerek által biztosított üzleti funkcionalitást, aminek valamilyen káros hatása lehet a rendszerek felhasználóira.
- **Incidens információra gyakorolt hatása:** az események befolyásolhatják a szervezet információinak titkosságát, sértetlenségét és rendelkezésre állását.
- **Incidensből helyreállíthatósága:** az esemény nagysága és az erőforrások típusa meghatározza, hogy mennyi időt és erőforrást kell fordítani az esemény helyreállítására.

... a három kombinációja adja meg végül is az adott eseménynél alkalmazandó prioritási sorrendet

2020.11.09.

ELTE IT Biztonság Speci

24

24

## Lehetséges prioritási kategóriák

Funkcionális hatás	
Kategória	Meghatározás
Nincs	Nincs hatással a szervezet azon képességére, hogy minden szolgáltatást minden felhasználó számára biztosítson
Alacsony	Minimális hatás; a szervezet továbbra is minden kritikus szolgáltatást megadhat minden felhasználó számára, de elvesztette a hatékonyságát
Közepes	A szervezet elvesztette a képességét, hogy kritikus szolgáltatást nyújtson a rendszert használók egy részének
Magas	A szervezet már nem képes kritikus szolgáltatásokat nyújtani egyetlen felhasználónak sem

Információra gyakorolt hatás	
Kategória	Meghatározás
Nincs	Semmilyen információt nem szűrték le, nem módosítottak, töröltek vagy más módon veszélyeztettek
Adatvédelmi jogsértés	Érzékeny, személyazonosításra alkalmas információhoz (PII) jutottak hozzá vagy szűrték meg őket
Tulajdonosi jogsértés	Osztályozatlan, saját tulajdonú információkhoz, például védett kritikus infrastruktúra-információkhoz (PCI) jutottak hozzá vagy szűrték le őket
Integritás elvesztése	Az érzékeny vagy védett információkat megváltoztattak vagy töröltek

2020.11.09.

ELTE IT Biztonság Speci

25

25

## Lehetséges prioritási kategóriák

Helyreállítási erőforrás	
Kategória	Meghatározás
Normál	A helyreállításhoz szükséges idő kiszámítható a meglévő erőforrásokkal
Bővített	A helyreállításhoz szükséges idő további erőforrásokkal meghatározható
Kiterjedt	A helyreállításhoz szükséges idő meghatározhatatlan; további forrásokra és külső segítségre van szükség
Nem lehet helyreállítani	Nincs lehetőség a helyreállításra (pl. érzékeny adatokat leszűrték és nyilvánosan közzé tették őket vagy visszaállíthatatlanul titkosítottak kritikus állományokat); vizsgálat indítása

2020.11.09.

ELTE IT Biztonság Speci

26

26

## Tájékoztatás

Amikor egy incidenst kielemezték és rangsorolnak, az incidens elhárító csoportnak **értesítenie kell a megfelelő személyeket**, hogy mindenki, akinek részt kell vennie, el tudja látni a szerepét:

- CIO
- Információbiztonsági vezető
- a szervezeten belül más eseményekre reagáló csapatok
- külső események elhárítási csoportjai (adott esetben)
- rendszergazda
- személyzeti / HR (alkalmazottakkal kapcsolatos esetek, például e-mailes zaklatás)
- külső tájékoztatás (olyan események esetén, amelyek nyilvánosságot generálhatnak)
- jogi osztály (esetleges jogi következményekkel járó események esetén)
- HunCERT, NKI
- hatóság (adott esetben)

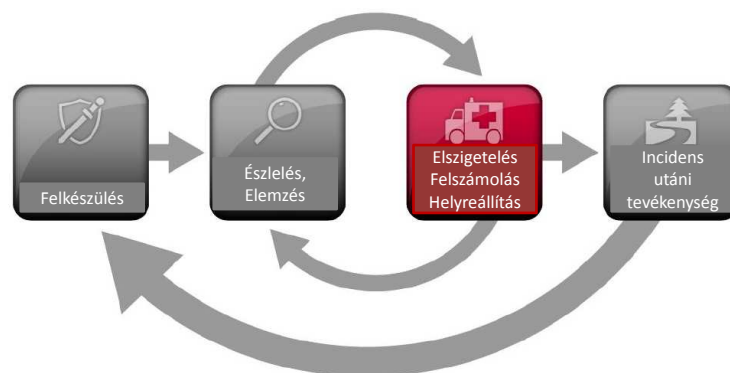
2020.11.09.

ELTE IT Biztonság Speci

27

27

## ... biztonsági incidens



2020.11.09.

ELTE IT Biztonság Speci

28

28

## Elszigetelési stratégia

- Az elszigetelés, leválasztás, karanténba helyezés rendkívül fontos, **mielőtt egy esemény kiterjedne** az összes erőforrásra, ezzel növelve a károkat.
- A legtöbb esemény **elszigetelést igényel**, ezért ez fontos szempont az egyes események kezelésének korai szakaszában.
- Az elszigetelés **időt biztosít** az adott eseményre szabott kármentesítési stratégia kidolgozására.
- A korlátozás elengedhetetlen része a **döntéshozatal** (pl. egy rendszer leállítása, leválasztása a hálózatról, bizonyos funkciók letiltása).
- Az ilyen döntéseket sokkal könnyebb meghozni, ha **vannak** előre meghatározott **stratégiák és eljárások** az incidens megfékezésére.
- A szervezeteknek meg kell határozniuk az **elfogadható kockázatokat** az incidensek kezelésében, és ennek megfelelően kell a kezelési stratégiákat kidolgozniuk.

2020.11.09.

ELTE IT Biztonság Speci

29

29

## Stratégia kritériumok

- Az erőforrások lehetséges **károsodása és eltulajdonítása**.
- A **bizonyítékok megőrzésének** szükségessége
- **Szolgáltatások elérhetősége** (pl. hálózati kapcsolat, külső feleknek nyújtott szolgáltatások)
- A stratégia megvalósításához **szükséges idő és erőforrások**
- A **stratégia hatékonysága** (például részleges elszigetelés, teljes elszigetelés)
- A **megoldás időtartama** (pl. sürgősségi megoldás négy órára, ideiglenes megoldás két hétig, tartós megoldás)..

2020.11.09.

ELTE IT Biztonság Speci

30

30

## Bizonyítékok összegyűjtése és kezelése

Az összes bizonyítékról részletes naplót kell vezetni, beleértve a következőket:

- **azonosító információk** (pl. a számítógép helye, sorozatszáma, modellszáma, host neve, MAC-címe és IP-címe);
- a nyomozás során a bizonyítékokat összegyűjtő vagy kezelő **személyek neve, beosztása és telefonszáma**;
- a bizonyíték kezelés minden előfordulásának **ideje és dátuma** (ideértve az időzónát is);
- a **bizonyítékok tárolási helyei**.

2020.11.09.

ELTE IT Biztonság Speci

31

31

## A támadók meghatározása

A támadó host **támadásakor leggyakrabban végrehajtandó tevékenységek**:

- a támadó **host IP-címének ellenőrzése**;
- a támadó **host kutatása** keresőmotorok segítségével;
- incidens **adatbázisok használata**;
- a lehetséges támadók **kommunikációs csatornáinak figyelése**.

2020.11.09.

ELTE IT Biztonság Speci

32

32



## Felszámolás

- Az esemény lokalizálása, kezelése után szükség lehet az esemény egyes **összetevői hatásának felszámolására, kiküszöbölésére** (pl. a rosszindulatú programok törlése, a korrumpált felhasználói fiókok letiltása, az összes kihasznált sebezhetőség azonosítása, stb.).
- A felszámolás során fontos **azonosítani** a szervezeten belül **az összes érintett host-ot**, hogy azokat azonnal kezelni lehessen.
- Egyes eseteknél a felszámolásra nincs szükség, vagy a helyreállítás során hajtják végre.

2020.11.09.

ELTE IT Biztonság Speci

33

33

## Helyreállítás

- A helyreállítás során az adminisztrátorok **visszaállítják a rendszer normál működését**, visszaigazolják, hogy a **rendszerek megfelelően működnek**, és (lehetőség esetén) **kezelik a biztonsági réseket** a hasonló események megelőzése érdekében.
- A helyreállításhoz tartozó további tevékenységek lehetnek még:
  - a rendszerek **helyreállítása tiszta biztonsági másolatokból**,
  - a rendszerek **újjaépítése alap helyzetről**,
  - a **sérült fájlok cseréje** tiszta verziókkal,
  - **javítások telepítése**,
  - **jelszavak megváltoztatása**,
  - hálózati eszközök **biztonságának szigorítása** (például tűzfalszabályok, routerek hozzáférési listáinak frissítése).
- A **magasabb szintű naplózás vagy a hálózat felügyelete** gyakran része a helyreállítási folyamatnak. Miután egy erőforrást sikeresen megtámadtak, gyakran újra megtámadják, vagy a szervezeten belül más erőforrásokat támadnak hasonló módon.

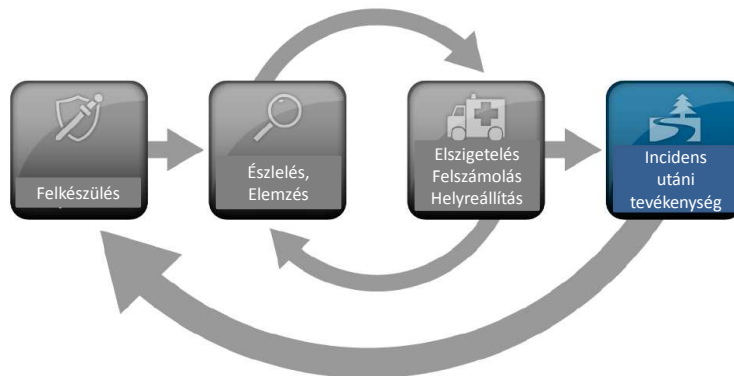
2020.11.09.

ELTE IT Biztonság Speci

34

34

## ... biztonsági incidens



2020.11.09.

ELTE IT Biztonság Speci

35

35

## Tanulás az eseményekből

- Pontosán mi történt, és mikor?
- Milyen volt a **teljesítménye a szervezetnek és a vezetésnek** az incidens kezelésében? A **dokumentált eljárásokat** követték? Azok **megfelelőek voltak**?
- Milyen **információkra** volt szükség hamarabb?
- Tettek-e olyan lépéseket vagy intézkedéseket, amelyek **gátolhatták** a helyreállítást?
- Mit csinálna **másképp** a szervezet és a vezetés, ha legközelebb hasonló esemény fordul elő?
- Hogyan lehetne **javítani az információk megosztását** más szervezetekkel?
- Milyen **javító intézkedésekkel** lehet megakadályozni a hasonló eseményeket a jövőben?
- **Milyen előre jelzőkre vagy indikátorokra** kell figyelni a jövőben a hasonló események felderítése érdekében?

2020.11.09.

ELTE IT Biztonság Speci

36

36

## Összegyűjtött incidens adatok felhasználása

- kezelt **incidensek száma**
- **felhasznált idők** incidensenként
- minden egyes incidens **objektív értékelése**
- minden egyes incidens **szubjektív értékelése** (incidens team)
- **adatok megőrzése**
- **költségek**

2020.11.09.

ELTE IT Biztonság Speci

37

37

## Szabványok, ajánlások

ISO/IEC 27000 standard family - information technology -  
Security techniques - Information security management  
systems requirements specification,  
ISO/IEC 20000 - IT Service Management;  
ITIL - Office of Government Commerce, IT Infrastructure  
Library, Service Management  
NIST - SP 800-61 Revision 2 - Computer Security Incident  
Handling Guide

2020.11.09.

ELTE IT Biztonság Speci

38

38

## Működésfolytonosság biztosításának információbiztonsági vonatkozásai

2020.11.09.

ELTE IT Biztonság Speci

39

39

## ISO - Fogalmak

Az **Üzletmenet Folytonossági Terv (ÜFT/BCP)** a szervezet üzleti folyamatainak fenntartására fókuszál működési zavarok alatt és után (pl. szervezet bérszámfejtési folyamata, számlázási folyamat). Az ÜFT vonatkozhat egyetlen szervezeti egység üzleti folyamatára, vagy a teljes szervezet összes folyamatára.

A **Katasztrófa Elhárítási Terv (KET/DRP)** a szolgáltatás súlyos, általában fizikai zavaraira vonatkozik, amelyek hosszabb ideig lehetetlenné teszik az elsődleges létesítmény-infrastruktúrához való hozzáférést. A KET egy információs rendszerre összpontosító terv, amelynek célja az alkalmazások vagy a számítógépes létesítmény infrastruktúrája működőképességének helyreállítása egy alternatív helyszínen vészhelyzet után.

2020.11.09.

ELTE IT Biztonság Speci

40

40

## ÜFT stratégia elemei

- annak meghatározása, hogy **mely üzleti célokat kell védeni**;
- melyik **veszteség / kár forgatókönyv a kritikus**;
- milyen típusú **üzleti leállások/megszakítások tekinthetők fenyegetésnek** a szervezet létére;
- **mennyire hajlandó a szervezet kockázatot vállalni** (kockázatvállalási hajlandóság), vagy mennyire magas a kockázatok elfogadottsága;
- **hogyan és milyen léptékben kell tenni valamit** ezzel kapcsolatban;
- mi az üzletmenet folytonosság irányítási rendszer **elsődleges célja**.

2020.11.09.

ELTE IT Biztonság Speci

41

41

## Fogalmak

Eszkálációs szint	Példák
Normál működés	-
Üzemzavar	Események, amelyeket jelenteni, ellenőrizni, dokumentálni és megszüntetni kell, amennyiben szükséges.
Korai figyelmeztetés	Olyan események, amelyek kezdetben védelmi vagy kockázatsökkentő intézkedéseket igényelnek csak, például egy helyi tűz eloltása.
Vészhelyzet	Olyan események, amelyek komolyan hátrányosan érintik az üzleti tevékenységet, és amelyeket a szükséges idő alatt már nem lehet megszüntetni.
Krízis	Olyan események, amelyek válságossá válhatnak, amelyek magasabb szintű koordinációt igényelnek, és amelyek életet veszélyeztethetnek vagy akár a szervezet létét.
Katasztrófa	Nagy kiterjedésű fizikailag káros események, amelyek nem csak a szervezetre korlátozódnak, alternatív helyszínre lehet szükség.

2020.11.09.

ELTE IT Biztonság Speci

42

42



43

## Fogalmak

Paraméterek	Meghatározás
Cél Helyreállítási Idő / Recovery Time Objective (RTO)	Meghatározza azt a <b>maximális időtartamot, ameddig a rendszer erőforrásai elérhetetlenek lehetnek</b> , még mielőtt ez elfogadhatatlan hatással lenne a többi rendszer erőforrására, a támogatott üzleti folyamatokra és az MTD-re.
Cél Helyreállítási Pont / Recovery Point Objective (RPO)	Az üzemzavar vagy a rendszer <b>leállása előtt azt az időpontot jelöli, amelyre a üzleti folyamat adatai visszaállíthatók</b> (ahol adva van az adatok legutolsó biztonsági mentése) kiesés után.
Maximálisan Eltűrhető Állásidő / Maximum Tolerable Downtime (MTD)	Azt az <b>időtartamot jelenti, amelyet a szervezet vezetése/szolgáltatás tulajdonosa hajlandó elfogadni</b> egy adott üzleti folyamat kiesése vagy megszakadása esetén, és minden ennek hatásával/következményével kapcsolatos körülményt tartalmaz.

2020.11.09. ELTE IT Biztonság Speci 44

44



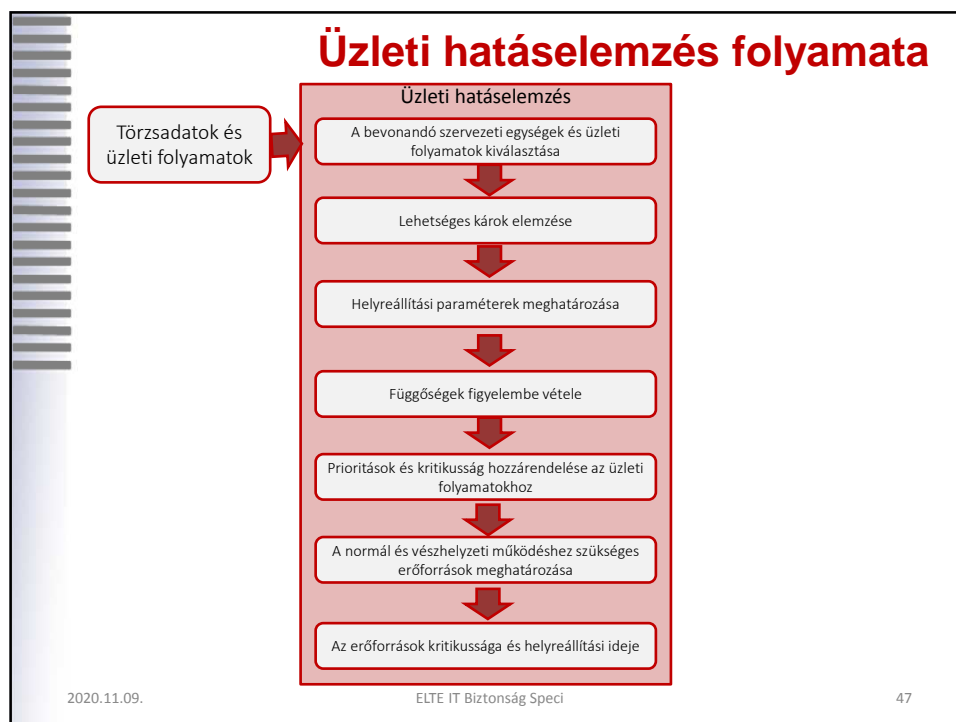
45

## Üzleti hatáselemzés (BIA) fogalmak

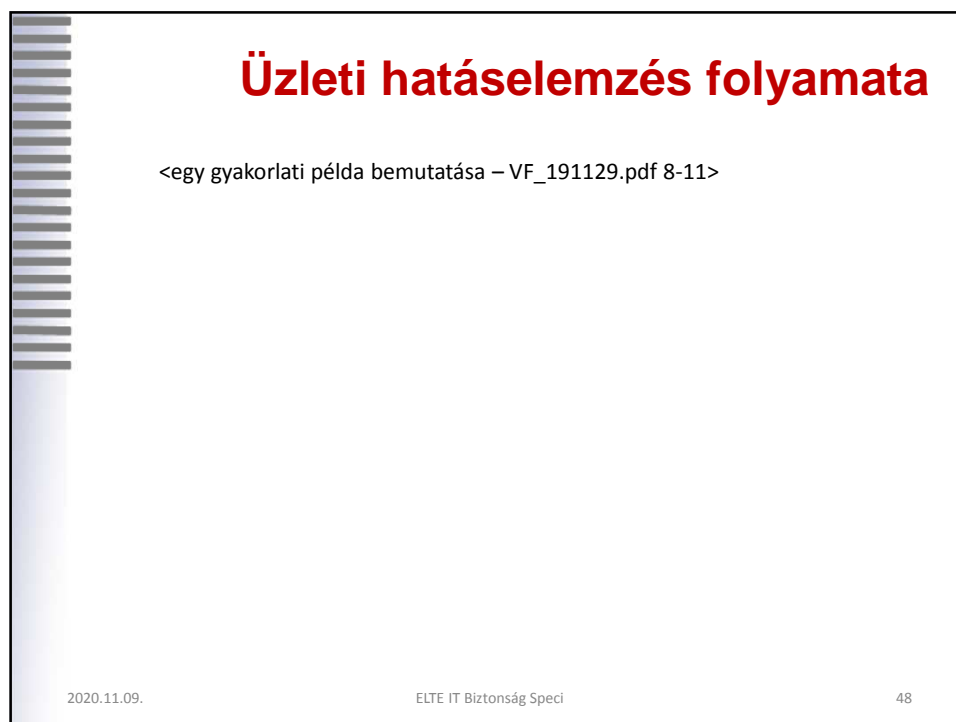
- Az üzleti hatáselemzés központi feladata annak megértése, hogy **mely üzleti folyamatok fontosak** az üzleti működés, tehát a szervezet fenntartása szempontjából, és az üzemzavar **milyen lehetséges következményekkel járhat**.
- Ezeknek a „kritikus” üzleti folyamatoknak az üzletmenet folytonosság kezelésekor **külön védelmet kell nyújtani**, és a vészhelyzet esetén célzott óvintézkedéseket kell tenni.
- A „kritikus” az üzletmenet folytonosság menedzsment szempontjából **„időkritikus”**-t jelent, ami azt jelenti, hogy ezt a folyamatot **gyorsabban kell helyreállítani**, mert különben nagy károk várhatók a szervezetben.
- Az ebből **eredő magas kár** anyagi veszteségekből, törvények vagy szerződések megsértéséből, jó hírnévből fakadó károkból vagy egyéb károkozásból állhat.
- A BIA által „nem kritikusnak” meghatározott üzleti folyamat nem azt jelenti, hogy ez a folyamat nem fontos a szervezet számára, hanem azt, hogy helyreállításának alacsonyabb prioritása van.

2020.11.09. ELTE IT Biztonság Speci 46

46



47



48



## Szabványok, ajánlások

ISO/IEC 27000 standard family - information technology - Security techniques - Information security management systems requirements specification,  
ISO/IEC 20000 - IT Service Management;  
ITIL - Office of Government Commerce, IT Infrastructure Library, Service Management  
BSI – Standard 100-4 Business Continuity Management  
NIST - SP 800-34 Rev. 1 - Contingency Planning Guide for Federal Information Systems

2020.11.09.

ELTE IT Biztonság Speci

49

49

## Naplózás és megfigyelés

2020.11.09.

ELTE IT Biztonság Speci

50

50

## Bemelegítés ...

- napló, log = események digitális lenyomata
- lényegében egyidős a számítástechnikával
- mindenhol jelen lehet ahol valamilyen számítógép alkalmazásra kerül
- napló lenyomat tartalma, szerkezete, felhasználási technikája, módja célhoz kötötten változhat

2020.11.09.

ELTE IT Biztonság Speci

51

51

## Definíciók

### Napló események digitális lenyomata

**Napló** egy szervezet rendszereiben és hálózataiban **előforduló események** a nyilvántartása. A **naplók** **naplóbejegyzésekből** állnak; minden bejegyzés információt tartalmaz egy adott eseményről, amely egy rendszeren vagy hálózaton belül történt.

NIST SP 800-92 - Guide to Computer Security Log Management

napló = log (mint technikai eszköz)

napló = audit (mint felhasználási cél)

2020.11.09.

ELTE IT Biztonság Speci

52

52

## Definíciók

A **bizonyíték** a rendszerek biztonsági ellenőrzésének fontos eszköze, hiszen az auditor **bizonyítékokat** keres a felvállalt kontrollok teljesítésének igazolásához.

pl.

szabvány: MSz ISO/IEC 27001

jogszabály: 2013. évi L. törvény (Ibtv.)

A **naplózás**, alapvető eszköz a **jogszabályi megfelelés bizonyítékainak** feltárásához, vizsgálatához

pl.

Európai parlament és a Tanács (EU) 2016/679 rendelete (GDPR)

2011. évi CXII. törvény - az információs önrendelkezési jogról és az információszabadságról

2020.11.09.

ELTE IT Biztonság Speci

53

53

## Naplózás alkalmazás

- **gyanús viselkedésnek** észlelése/nyomon követése
- ipari **ágazati támadások** (egészségügyi vészjelzés, pénzügyi csalás) észlelése
- külső és belső **fenyegetettségek** feltárása
- **monitorozás**: pl. felhasználói tevékenység, szerverek és adatbázis elérések, felhő és helyi infrastruktúrák kombinációjának
- IT/hálózati rutin **karbantartások** támogatása
- analízisi és szervezési támogatás **biztosítása** incidens helyzetek kezeléséhez
- **biztonsági vizsgálat** támogatása
- **hibaelhárítás**
- **megfelelőségi riportok** biztosítása
- analízisi és szervezési támogatás biztosítása incidens helyzetek kezeléséhez

2020.11.09.

ELTE IT Biztonság Speci

54

54

## Naplózás forrásai (Log források)

- Biztonsági alkalmazások naplóállományai
- Operációs rendszerek naplóállományai
- Alkalmazások naplóállományai

2020.11.09.

ELTE IT Biztonság Speci

55

55

## Biztonsági alkalmazások naplóállományai

... amelyek elsődlegesen informatikai biztonsággal kapcsolatos bejegyzéseket tartalmaznak:

- Antimalware alkalmazás (pl. anivírus SW-k)
- Behatolás-érzékelő (IDS) és a behatolás-megelőző (IPS)
- Távoli elérésű szoftver (pl. VPN rendszerek általában naplózzák a sikeres és sikertelen bejelentkezési kísérleteket)
- Web proxy-k
- Authentikációs szerverek
- Router-ek
- Tűzfalak
- Hálózati karantén szerverek

2020.11.09.

ELTE IT Biztonság Speci

56

56

## Operációs rendszerek naplóállományai:

... szerverek, munkaállomások és hálózati eszközök (pl. router-ek, switch-ek) operációs rendszerei (OS) általában különféle a biztonsággal kapcsolatos információkat tartalmaznak:

- **rendszer események:** olyan operációs műveletek, amelyeket az operációs rendszer alkotóelemei hajtanak végre, például a rendszer leállítása vagy a szolgáltatás indítása, általában a jelentős sikeres és sikertelen eseményeket naplózása, de sok operációs rendszer lehetővé teszi az adminisztrátoroknak, hogy meghatározzák, melyik típusú események legyenek naplózva;
- **audit bejegyzések:** olyan biztonsági eseményekkel kapcsolatos információkat tartalmaznak, mint a sikeres és sikertelen hitelesítési kísérletek, a fájlhozzáférések, a biztonsági házirendek változásai, a fiókváltozások (például a fiók létrehozása és törlése, a fiókjogosultságok hozzárendelése) és a jogosultságok használata.

2020.11.09.

ELTE IT Biztonság Speci

57

57

## Alkalmazások naplóállományai

... kereskedelemben kapható felhasználásra kész adott funkcionálitással bíró vagy integrált rendszerek. A leggyakrabban naplózott információ típusok:

- **kliens kérések és szerver válaszok**, amelyek nagyon hasznosak lehetnek az eseménysorozat rekonstruálásában és a látszólagos eredmény meghatározásában (pl. e-mail szerverek, amelyek rögzítik az egyes e-mailek feladóját, a címzettet, a tárgyat és a mellékletek azonosítóit);
- **felhasználói fiók információk**, például sikeres és sikertelen hitelesítési kísérletek, fiókváltások (pl. fiók létrehozása és törlése, fiókjogosultságok kiosztása);
- **használati információk**, például egy adott időszakban végrehajtott tranzakciók száma, a tranzakciók mérete (pl. e-mail üzenet mérete, fájlátvitel mérete);
- **jelentős üzemeltetési tevékenységek** (pl. alkalmazás indítása és leállítása, hibái, alkalmazás konfigurációjának jelentős változásai).

2020.11.09.

ELTE IT Biztonság Speci

58

58

## Naplózó infrastruktúrák

... alapvetően az alábbi három réteget tartalmazzák:

- **naplóbejegyzés generálás:** az első szintet képviselik a host-ok, amelyek a naplóbejegyzéseket generálják;
- **naplóbejegyzés analízálás és tárolás:** a második szinten lehet egy vagy több naplószerver, melyek megkapják a napló adatokat, azok másolatát az első szinten lévő host-okról;
- **napló monitorozás:** a harmadik szinten konzolok találhatók, melyek monitorozzák és átvizsgálják a naplózandó, illetve előzőleg automatikusan analízált adatokat.

2020.11.09.

ELTE IT Biztonság Speci

59

59

## Naplózó infrastruktúrák funkciói

- Általános alapfunkciók
- Tárolás
- Analízálás
- Megsemmisítés

2020.11.09.

ELTE IT Biztonság Speci

60

60

## Általános alapfunkciók

- **parse-olás:** adatok kivétele a naplóbejegyzésből, mely adatok aztán más formában felhasználhatók másik naplózási folyamatban vagy további naplózási funkciók részeként, mint például konverzió és megtekintés;
- **eseményszűrés:** felesleges naplóbejegyzések elhagyása, melyek nem tartalmaznak olyan információt, amelyre akár analízis, riportkészítés vagy hosszabb távú tárolás esetén lenne szükség;
- **esemény aggregálás:** során az azonos tartalmú naplóbejegyzések egyetlen konszolidált naplóbejegyzést eredményeznek az eseményről, azonban az előfordulások számossága is rögzítésre kerül.

2020.11.09.

ELTE IT Biztonság Speci

61

61

## Tárolás

- **naplófájl rotáció:** azaz lezárásra kerül egy naplófájl és egy következő megnyitásra kerül;
- **naplóállományok archiválása:** célja a hosszú távú megőrzés megadott időtartamra valamilyen hordozható médián;
- **naplóállomány tömörítés:** tárolási céllal azért, hogy fizikailag kisebb helyet foglaljon el;
- **napló redukálás:** a szükségtelen tartalom elhagyását jelenti;
- **napló konverzió:** parse-olásra kerül az analizálásra szánt tartalom, majd ezt a tartalmat eltárolják egy másik formátumban;
- **adat normalizáció:** minden naplóbejegyzés konvertálásra kerül valamilyen adat reprezentációra, melyek be lesznek kategorizálva (pl. időpont megadás formátumok, illetve az időzónák használata);
- **naplófájl integritás ellenőrzése:** lenyomat készül minden fájlról, melyet biztonságos módon (titkosítva) eltárolnak, ezzel garantálva a fájl sértetlenségét.

2020.11.09.

ELTE IT Biztonság Speci

62

62

## Analizálás, Megsemmisítés

- **esemény korreláció:** kapcsolatokat keresnek az egyes bejegyzések között, leggyakoribb módszer valamilyen szabályalapú megfeleltetés, lehet több forrásban keresni ugyanazt a mintát, vagy egy forrásban a több előfordulást;
- **napló megtekintése:** humán feladat, ezért az egyes bejegyzések valamilyen olvasható formában jelennek meg;
- **napló riportok készítése:** során a naplóelemzés eredménye jelenik meg valamilyen formában.
- **napló törlés:** során az összes bejegyzés törlésre kerül, ami történhet megadott időben, megadott időközönként

2020.11.09.

ELTE IT Biztonság Speci

63

63

## Syslog alapú központosított naplózó alkalmazás

- első, általánosságban használt technológia,
- csak alapvető biztonsági kontrollokkal rendelkezik a bizalmasság, sértetlenség, illetve a rendelkezésre állás tekintetében, (pl. UDP protokoll használata, nincs titkosítás, stb.),
- RFC 3195 szerinti megerősítések:
  - megbízható napló továbbítás, azaz az UDP protokoll kiegészült a TCP protokoll alkalmazásával,
  - az átvitel titkosságának védelme a TLS használatával,
  - az átvitel sértetlenségének védelme és autentikálás, azaz titkosított lenyomat SHA-1 alkalmazásával;
- további funkció javítások: kiterjedt szűrés, log elemzési lehetőségek, több üzenet formátum, tárolási lehetőség adatbázisban, méret behatárolás.

2020.11.09.

ELTE IT Biztonság Speci

64

64



## SIEM - Security Information and Event Management

- Biztonsági Információ és Esemény Menedzsment rendszer;
- mára a legelterjedtebb;
- egy vagy több naplószervert tartalmazhatnak log analízálásra;
- egy vagy több adatbázis szervert a naplók tárolására;
- legtöbb SIEM termék két lehetőséget biztosít naplóbejegyzések gyűjtésére és analízálására:
  - ügynök nélküli: ebben az esetben a SIEM szerver olyan log-okat gyűjt, amelyek önálló host-on kerülnek generálásra anélkül, hogy azokra valamilyen speciális alkalmazást telepítenének;
  - ügynök alapú: valamilyen ügynök alkalmazás kerül telepítésre a log-ot generáló host-ra, amelyik végrehajtja az esemény szűrést, aggregálást, normalizációt a naplóbejegyzések egy részén, majd a normalizált naplóbejegyzések átvitelre kerülnek a SIEM szerverre rendszerint valós időben;
- néhány SIEM szerver képes alkalmazni akár syslog, SNMP, JDBC vagy egyéb alkalmas formátumot is.

2020.11.09.

ELTE IT Biztonság Speci

65

65

## SIEM és Log Management\* eszközök összehasonlítása

Funkcionalitás	SIEM	LM
adat típus	széles választék	széles választék, de néha ez korlátozott
normalizáció	rendszerint erős	rendszerint egyszerű
adattárolás	kereskedelemben kaphatók vagy egyedi	rendszerint egyedi
korreláció	erős	egyszerű/nincs
valós idejű riasztási lehetőség	kiváló	alig vagy nincs
trend vizsgálat historikusan	jótól kiválóig	aligtól jóig
ad-hoc lekérdezés	aligtól jóig	kiváló
riportok	jótól kiválóig	jótól kiválóig
esemény felvételi sebesség	aligtól jóig	jótól kiválóig
strukturált lekérdezés sebessége	aligtól jóig	jótól kiválóig
strukturálatlan (full-text) lekérdezés sebessége	nemtől szegényes	jótól kiválóig
kliens interfész	komplex/teljes funkcionalitású, Java vagy Web 2.0 alapú	egyszerűtől komplex Web 2.0 alapig
kiszérelés	szoftver, virtuális appliance, hardver appliance	szoftver, virtuális appliance, hardver appliance

**Log Management:** szakirodalomban általánosan használt elnevezés a nem SIEM és inkább Syslog alapú naplózó rendszerekre

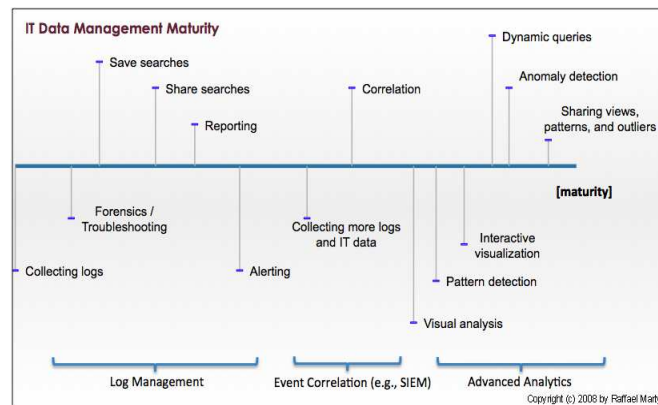
2020.11.09.

ELTE IT Biztonság Speci

66

66

## Naplózó infrastruktúrák érettségi modellje



2020.11.09.

ELTE IT Biztonság Speci

67

67

## Naplózó rendszerek használata

Rendszertermek legalább az alábbiakat kell tartalmazni:

- **naplózó források**
  - biztonsági alkalmazások (host-ok) listája (3.1 Biztonsági alkalmazások fejezet szerint),
  - operációs rendszer (szerverek, munkaállomások, hálózati eszközök, stb.),
  - egyéb alkalmazások,
  - naplózandó eseménytípusokat (biztonsági események, hálózati események, stb.),
  - naplóbejegyzések tartalma,
  - naplóbejegyzések gyakorisága,
- **naplóbejegyzések továbbítása**
  - központi naplózó infrastruktúrába továbbító források,
  - naplózó infrastruktúrába továbbítandó bejegyzések típusai
  - továbbítás módjai (útvonalak, protokollok, stb.),
  - hálózati eszközök kezelésének módja,
  - továbbítások gyakorisága (real-time vagy ütemezetten),
  - naplóforgalom védelme (sértetlenség, bizalmasság és rendelkezésre állás),

2020.11.09.

ELTE IT Biztonság Speci

68

68

## Naplózó rendszerek alkalmazásba vétele

- **naplóállományok tárolása és törlése**
  - naplóállományok rotálásának rendje,
  - naplóállományok védelme (bizalmasság, sértetlenség és rendelkezésre állás),
  - naplóbejegyzések megőrzési időtartama,
  - szükségtelen naplóállomány megsemmisítési módja, eljárása,
  - naplóállományok tárolási kapacitása,
  - naplóbejegyzések bizonyító módjának biztosítása,
- **naplóelemzés**
  - naplóelemzést gyakorisága, üteme,
  - naplóelemzés jogosultsági rendje (ki, mikor, hogyan, miért, stb.), ennek naplózása,
  - azonosított vagy gyanított esemény kezelésének rendje (esetleg létező incidens kezelési eljárásba integrálás),
  - naplóelemzés eredményének védelme (bizalmasság, sértetlenség és rendelkezésre állás),
  - érzékeny adatok (személyes adatok, e-mail-lel) naplózhatóságának feltételei, körülményei.

2020.11.09.

ELTE IT Biztonság Speci

69

69

## Naplózó rendszerek használatának korlátai

- megfelelő szakképzettség/tudás hiánya,
- szabályok manuális létrehozásának, finomításának szükségessége,
- pénzhiány,
- túl sok false-positives jelzés,
- rendszer komplexitása,
- a biztonsági eszközök átfogó ismeretének hiánya,
- vállalati kultúra,
- alkalmazottak biztonsági tudatosságának hiánya,
- a megoldás telepítésének a bonyolultsága,
- a menedzsment támogatás, biztonság tudatosság hiánya,
- hálózati forgalom és bizonyos egyéb folyamatok láthatóságának hiánya,
- az egyes biztonsági megoldások szegényes integráltsága,
- az elérhető eszközök alkalmatlansága, használhatatlansága,
- szegényes szállítói támogatás,
- hatékony eszköz hiánya a piacon.

2020.11.09.

ELTE IT Biztonság Speci

70

70

## Szabványok, ajánlások, irodalom

- Common Criteria (ISO/IEC 15408)
- ITIL (ISO/IEC 20000)
- COBIT
- ISO/IEC 2700x szabványcsalád
- NIST SP 800-92 - Guide to Computer Security Log Management
- Giesz István: Szakdolgozat/METU - Különböző típusú naplók gyűjtésének és elemzésének előnyei és korlátjai az informatikai rendszerekben

2020.11.09.

ELTE IT Biztonság Speci

71