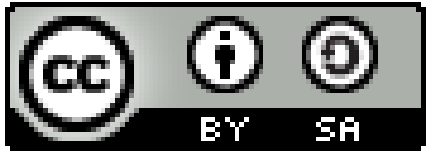
Biztonsági incidensek fogalma, kezelése



Bisztray Frigyes
HunCERT

HUNCERT

Információ biztonság

- Biztonság
  - Az élet minden területén → Információ biztonság
    - Preservation of confidentiality, integrity and availability of information. In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can be involved.
- Növekvő igény
  - Digitalizálódás
  - Jó buzzword
- Növekvő követelmény
  - Törvényi előírások
- Növekvő ráfordítás
  - Virusirtótól a SOC-ig

Fogalmak:

- Esemény, Szabálytalanság, Incidens, Riasztás, Értesítés, Megsértés, Hiba

Fogalom meghatározások

- Eltérő meghatározások:
  - Szervezetek
    - CERT
    - NIST
    - SANS
  - Szabványok
    - ISO 27001
  - Országok (EU)
    - Törvények
  - Szakértők

Event

- Event - esemény
  - ISO 27001
    - „Any occurrence related to assets or the environment indicating a possible compromise of policies or failure of controls, or an unmapped situation that can impact security.”
  - ENISA
    - „Any occurrence that may lead to a Business Continuity incident”
  - SANS
    - „An event is an observable occurrence in an information system that actually happened at some point in time.”

Event

- Event - esemény
  - ITIL
    - “An event can be defined as any detectable or discernible occurrence that has significance for the management of the IT Infrastructure or the delivery of IT service and evaluation of the impact a deviation might cause to the services. Events are typically notifications created by an IT service, Configuration Item (CI) or monitoring tool.”
  - NIST
    - „An EVENT is any observable occurrence in a system or network”

Event

- Esemény:
  - Egy email
  - Egy telefon hívás
  - Egy rendszer összeomlás
  - Egy fájlra vonatkozó vírus ellenőrzés kérés
  - …
- observable ↔ non observable?
- possible compromise of policies
- compromise ↔ any occurence
-

Incident

- Incident - Incidens
  - ISO 27001
    - „One or more information security events that compromise business operations and information security.”
  - ENISA – ITIL
    - „Any event that is not part of the standard operation of a service and that causes, or may cause, an interruption to, or a reduction in, the quality of that service”
  - SANS
    - „An incident is an adverse event in an information system – includes the significant threat of an adverse event. In another word, it implies harm or the attempt to harm.”
  -

Incident

- Incident:
  - violation of an explicit or implied security policy
  - the attempts to gain unauthorized access
  - unwanted denial of resources
  - unauthorized use
  - changes without the owner's knowledge, instruction, or consent
  - …
- something that in fact negatively affect the business or information which should be protected
- Minden incidens esemény, de nem minden esemény incidens

Non-complience

- Non-compliance
  - ISO 27001
    - „any situation where a requirement is not being fulfilled”
      - Pl. backup copies are not being generated as defined in the Backup Policy
  - …
- something you should be doing, but are not

Alert

- Alert – Riasztás?
  - ENISA
    - „A formal notification that an incident has occurred which may develop into a Business Continuity Management or Crisis Management invocation”
  - ITIL
    - Categorization based on the significance of an event (INFO/WARN/ALERT/ERROR)
  - Event notification = Alert ?
    - An alert is a notification that a particular event (or series of events) has occurred, which is sent to responsible parties for the purpose of spawning action.
  -

Alert

- An event will happen. It happens even if it is not detected and flagged. An alert is when a monitoring system detects it and raises this fact somewhere for further processing (and potentially triggers a notification as well). So an Alert is always in response to an event (in other words there is always an event with an alert) but there is not always an alert with an event.”

Notification

- Notification - Értesítés
  - notifications bring alerts and incidents to the attention of people that need to act and to respond.

Breach

- Breach – Megsértés
  - Technopedia
    - A security breach is any incident that results in unauthorized access of data, applications, services, networks and/or devices by bypassing their underlying security mechanisms. A security breach occurs when an individual or an application illegitimately enters a private, confidential or unauthorized logical IT perimeter.
  - CyberShark
    - If a security incident results in unauthorized access to data, it can typically be classified as a security breach. The precise definition of a data breach varies depending on the laws that apply to your organization.
  - GDPR – personal data breach
    - "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."

Érzékelési folyamat

- Eltérő meghatározások oka a folyamat különböző szempontok szerinti megközelítése
  - Történik valami
  - Ezt érzékeli valami, valaki
  - Kezdeti szűrés
  - Értesíti az illetékest (személyt, programot)
  - Kiértékelés, osztályozás
  - Kiértékelés eredménye alapján a szükséges válaszlépések elindítása
  - Különböző törvények, szabályozások, biztonsági házirendek
    - Más más célterület
  - Az egyes fogalmakat az adott környezetükben kell/lehet meghatározni/értelmezni
  -

Esemény, Incidens - Sztaki

- Esemény
  - A biztonságot érintő, azzal kapcsolatba hozható történés, ami magában hordozza a biztonság esetleges sérülésének lehetőségét
    - Indokolatlanul sok bejelentkezés
    - Ismeretlen személy a gépterem folyosóján
- Incidens
  - Az esemény negatívan befolyásolja a biztonságot
    - Illetéktelen belépési kisérlet
    - Behatolási kisérlet a gépterembe

Esemény, Incidens kezelése

- Az esemény, incidens kezelés fő lépései:
  - Behatárolás
    - Karantén
    - Rögzítés
    - Kiértékelés
  - Kiírtás, elhárítás
  - Helyreállítás
  - Felülvizsgálat
  - Időközönkénti felülvizsgálat

Esemény, Incidens rögzítése

- Behatárolás
  - Rögzítés
    - Alap adatok
      - Dátum
      - Idő
      - A bejelentés forrása (ki, mi)
      - Esemény leírása
    - Leghasznosabb
      - Log-ok
    - IDS használata esetén
      - A (látszólagos) forrás cím
      - Cél cím
      - Az IDS rendszer által kiadott risztások
      - Az érzékelő(k) helye
      - Az eseményhez kapcsolódó első risztás ideje
      - Az eseményhez kapcsolódó utolsó riasztás ideje

Esemény, Incidens kiértékelése

- Kiértékelés
  - Szükséges reakció meghatározása
    - Cél: Csak a szükséges erőforrás ráfordítás
  - Esemény osztályozása
    - Incidens?
      - Veszélyezteti az adatok integritását?
      - Veszélyezteti az erőforrások rendelkezésre állását?
      - Veszélyezteti az adatok bizalmasságát?
      - A tevékenység abnormális?
      - Sérti a vállalat/szervezet biztonsági előírásait?
    - Súlyosság
    - Típus
  - Eszkaláció
    - Az illetékesek értesítése

Esemény, Incidens kezelése

- Kiírtás, elhárítás
  - Az eseményt kiváltó okok megszüntetése
    - pl. Vírus irtás, rendszer frissítés, tűzfal módosítás, jelszó csere
- Helyreállítás
  - Az eredeti adatok visszaállítása (a rendszer remélhetőleg már biztonságosabb)
- Felülvizsgálat
  - Az elvégzett intézkedések eredményének ellenőrzése
  - A jövőbeni ismétlődés elkerülése – megelőző intézkedések
  - Az elvégzett intézekedések folyamatának ellenőrzése
  - Az incidens kezelési folyamat javítása

Kérdések?

Köszönjük a figyelmet!

http://www.cert.hu
cert@cert.hu