Basque CyberSecurity Centre

Kalteberatasunen kudeaketa cheat sheet

1. Definizioa

Prozesu horren bidez, erakunde bateko sistemek eta softwareak dituen segurtasuneko arriskuak identifikatzen eta ebaluatzen dira, eta horien berri ematen da. ***"Vulnerability Management"*** deitzen zaio prozesu horri.

Prozesu horrek, segurtasuneko beste neurri batzuekin identifikatuta, eraso posibleen iturriak "kontrolatuta" izatea ahalbidetzen die erakundeei. Hala, arreta gune horietako segurtasuna sendotzen ezar dezakete.

Kudeaketa-plana aldizkakotasunez berrikusi eta eguneratu behar du goi mailako zuzendaritzak. Horrek erakundearen datuen babesa hobetzen lagunduko luke.

2. Kudeaketa-prozesua

Identifikazioa

Urrats kritikoa. Identifikazio ona funtsezkoa da mehatxuak aztertzeko eta arintzeko kontrolak ezartzeko.

Kalteberatasunak identifikatzeko tresnak/aukerak:

Sarearen eskanerrak. Konektatutako sistema guztiak identifikatzen eta kalteberatasunen bila aztertzen dituzte.

- **Nola?** TCP/UDP paketeak bidalita edo PINGak gauzatuta.
- **Mota:** Barnekoak (saretik egindako erasoak eta probak) eta kanpokoak (ikerlari batek kanpotik egindako erasoa simulatzen du).
- **Tresnak.** Nmap, OpenVAS, ...

Agenteak instalatzea. Gailuaren etengabeko monitorizazioa. Txostenak sortzea eta metrikak lortzea errazten dute.

- **Nola?** Gailuan agentea instalatuta.
- **Tresnak.** Kismet, Tenable, ...

Ebaluazioa

Kalteberatasunak eta lotura duen informazioa identifikatutakoan, balorazio-prozesua hasten da. Lehentasunak finkatzeko eta arreta erakundearen jarraipena arriskuan jar dezaketen arriskuetan jartzeko, beharrezkoa izango da topatutako ahulezia bakoitza ebaluatzea.

- Egon daitezkeen positibo faltsuak desagerrarazita, emaitzak berrikustea.
- Ebaluazio-sistema bat erabiltzea: probabilitatea/inpaktua matrizea, adibidez.
  - Arrisku kritikoak modu bisualean identifikatzea errazten du.
  - Mehatxuak erakundean izan dezakeen eraginaren eta gertatzeko probabilitatearen arabera sailkatzea.
  - Arrisku-atalase onargarria finkatzea.

PROBABILITATE-INPAKTU MATRIZEA		**INPAKTU**				
		Oso txikia (0.1)	Txikia (0.2)	Ertaina (0.3)	Handia (0.4)	Oso handia (0.5)
PROBABILITATE	Oso txikia (0.1)					D 0.05
	Txikia (0.2)	C 0.02			B 0.08	
	Ertaina (0.3)	E 0.03				
	Handia (0.4)	A 0.04				
	Oso handia (0.5)					

Basque CyberSecurity Centre

Kalteberatasunen tratamendua

Tratamendu-estrategia aukeratzea:

- **Arriskua ekiditea edo desagerraraztea.** Arriskua eragiten duen aktiboa desagerrarazita, mehatxua desagertu egingo da.
- **Arriskua arintzea.** Arriskua maila onargarriraino gutxitzeko neurriak edo kontrolak aplikatzea.
- **Arriskuaren transferentzia.** Arriskua hirugarren bati edo erakunde bati transferitzea.
- **Arriskua onartzea.** Arriskua hor dagoela onartzea eta ezer ez egitea. Erabilgarria da kalteberatasun bat arrisku baxukotzat jo denean eta hori zuzentzearen kostua izango lukeen eragina baino askoz ere handiagoa bada.
- **Arriskua erremediatzea.** Ahal den neurrian, kalteberatasuna konpontzea edo adabakia jartzea.

Tratamendua osatu denean, kalteberatasunaren beste azterketa bat gauzatuta, hori egiaztatzea komeni da arindu edo erremediatu dela bermatzeko.

Jakinarazpena

Emaitzen txostena sortzea

Kalteberatasunen azterketako emaitzek erakundean argitaratuta egon behar dute honako hauek lortzeko:

- Arriskuen inguruko kontzientzia sortzea.
- Etorkizuneko arriskuak identifikatzea erraztea.
- Arriskuak saihesteko neurriak, teknikak eta tresnak ezartzea.
- Arriskuen zergatia ulertzea.

Erremediatzeko plana sortzea

Probabilitatea/inpaktua matrizearekin ezarritako lehentasunaren arabera, identifikatutako eta ebaluatutako alderdiak zuzentzea ahalbidetuko lukeen kalteberatasunen kudeaketa-plana garatzea eta gauzatzea.

3. Tresnak

Erakundearen segurtasunean eragina izan dezaketen kalteberatasunen bila edozein sare edo sistema modu automatikoan aztertzeko diseinatutako softwarea.

NMAP

- Tokiko sare baten barruan host-ak identifikatzeko gehien erabiltzen den tresna da. Interneten hostak identifikatzea ere ahalbidetzen du, sarera konektatuta dauden egiaztatzeko.
- Atakak eskaneatzea ahalbidetzen du FWko babesik gabeko zerbitzu eragileak identifikatu ahal izateko.
- Kode irekia eta plataforma anitzekoa. Pentesting gisa Linux erabiltzea da ohikoagoa

OpenVAS

- Aztertu beharreko sare barruan eta kanpoan gauzatzea ahalbidetzen du, kanpoko erasoa simulatuta.
- Identifikatutako kalteberatasunak eta gure sistemarako arriskuak xehetasun osoz jasotzen dituen txostena sortzen du.
- Etengabeko monitorizaziorako konfiguratzea ahalbidetzen du, atalaseak eta alertak ezarrita.

Tenable (Nessus)

- Agenteetan oinarrituta dago.
- Kalteberatasunen, konfigurazio okerren (CIS erreferentzien konfigurazioa betetzea) eta sistemako datuen inguruko informazioa biltzen dute eta, gero, informazio hori Nessus Manager-i edo Tenable.io-ri bideratzen diote hark azter dezan.
- Aginte-koadroak eskaintzen ditu emaitzak jakinarazteko monitorizazioa eta txostenaren txantiloiak egiteko.