ZIBERSEGURTASUN TAXONOMIAK

EDUKIEN TAULA

1. TAXONOMIAREN AZALPENA

Proposatutako zibersegurtasun taxonomiak hainbat maila ezartzen ditu. Horien bidez, produktu eta zerbitzuei dagozkienak soilik bereiz ditzakegu.

Sailkapen horrek aukera ematen du egun zibersegurtasunaren merkatuan dauden zerbitzu eta produktuak ondo ezagutzeko. Horrela, produktu eta zerbitzuen irismenaren arabera, bakoitzari eragiten dioten arlo nagusiak identifika ditzakegu.

Bestalde, taxonomiaren bidez, zehatz dezakegu nori bideratuta dauden konponbide eta produktuak.

Irismen horiekin, bilaketa eta sailkapenak erraz egin ditzakegu; izan ere, kategoriak erabiltzeaz gain, aplikatu nahi den arlo edo eremuaren arabera egin daitezke bilaketak.

Konponbide horietarako aplikazio eremuak honakoak dira:

- Startup
  - Negozio berri bati ekin nahi dioten enpresak dira; hastapen edo eraikuntza fasean dauden negozio-ideien inguruan lan egiten dute.
- Mikroenpresa
  - 10 langile baino gutxiagoko enpresak; edo, kasu askotan, autonomoak.
- ETE
  - 10 eta 250 langile bitartean dituzten enpresak, tarteko negozio bolumenarekin.
- Enpresa handia
  - 250 langiletik gorako enpresak, azpiegitura propioekin eta negozio bolumen handiarekin.

Aurretik azaldutako guztiaren ondorioz, taxonomiaren azken eredua ematen da. Batetik, zibersegurtasun produktuen kategoriari dagozkion elementuak erakusten dira, eta bakoitzari eragiten dioten aplikazio eremuak:

PRODUKTU KATEGORIA		APLIKAZIO EREMUA				
		Sarbide eta nortasun kudeaketa	Lanpostuko segurtasuna	Aplikazio eta datuen segurtasuna	Sistemen segurtasuna	Sareko segurtasuna
	Iruzurraren aurkakoa		☑	☑	☑	☑
	Malwareen aurkakoa		☑	☑	☑	☑
	Ikuskaritza teknikoa	☑		☑		☑
	Araudi ziurtagiria		☑	☑	☑	☑
	Kontingentzia eta jarraitutasuna		☑	☑	☑	☑
	Sarbide eta egiaztatze kontrola	☑				
	Legea betetzea	☑	☑	☑		
	Segurtasun adimena			☑	☑	☑
	Informazio-ihesaren prebentzioa		☑	☑		☑
	Jakinarazpenen babesa		☑	☑	☑	☑
	Gailu mugikorren segurtasuna		☑			☑

Ondoren, aurretik erakutsitako elementu bakoitzaren azalpen laburra emango da:

- **Iruzurraren aurkakoa:** Phishing teknikaren bidez, mezu elektronikoen edo horretarako bereziki diseinatutako malwareen bidez informazioa lapurtu edo identitatea faltsutzeko ekintzen aurka babesteko konponbideak.
- **Malwareen aurkakoa:** Birus, troiar, spyware eta antzeko software maltzurren aurrean sistema informatikoak (zerbitzariak, ordenagailuak, eramangarriak, mugikorrak eta abar) babestera bideratutako tresnak.
    - Beren funtzioa software maltzurra atzeman eta ezabatzea da, ekipoa infektatzera heldu aurretik.
- **Ikuskaritza teknikoa:** Segurtasuna errebisatu eta ebaluatzeko tresnak, arlo tekniko, teknologiko eta antolakuntza arlo guztiak kontuan hartuz; orokorrean, estandar bat hartzen da erreferentzia moduan. Helburua sistema, aplikazio eta datuen ikuskaritzak egitea da, segurtasun arloan egon daitezkeen ahultasun posibleak antzemateko.
- **Araudi ziurtagiria:** Arau horien inguruko ziurtagiriak lortu eta segurtasun arloko araudia betetzen dela bermatzeko tresnak. Segurtasun politikak ezartzeko, segurtasun-neurriak aplikatzeko, aktiboak baloratzeko eta abar erabiltzen dira.
- **Kontingentzia eta jarraitutasuna:** Ekintza eta kontingentzia planak egiteko tresnak, betiere, segurtasun arloko edozein gertakarik sortutako eraginak arintze aldera. Erakunde batean egon daitezkeen segurtasun istripuen aurrean kritikotzat hartzen diren sistema edo prozesuak berreskuratzera bideratuta daude. Lainoko sistemak, birtualizazio edo urrutiko backup konponbideak dira irtenbideetako batzuk.
- **Sarbide eta egiaztatze kontrola:** Mekanismo enpresetan ezartzera bideratutako produktuak, erabiltzaileak eta baimenak kudeatu edota baliabideetarako sarbidea kontrolatzeko. Horretarako, egiaztatze mekanismoak eta baliabide digitalen erabilerara bideratutako tresnak erabiltzen dira.
- **Legea betetzea:** Informazioaren segurtasunaren inguruan legea betetzen laguntzen duten tresnak, hala nola DBAOren kasuan (Datuen Babeserako Araudi Orokorra), merkataritza elektronikoa eta abar.
- **Segurtasun adimena:** Zibersegurtasun arloko ekitaldi edo istripuak kudeatzeko fluxu bat ezartzeko aukera ematen duten tresnak, ahalik eta denbora laburrenean arintzeko asmoz.
- **Informazio-ihesaren prebentzioa:** Informazioaren konfidentzialtasuna, eskuragarritasuna eta integritatea ziurtatzeko tresnak. Helburu nagusia zera da: informazio-galera saihestu eta informazio-ihesak identifikatu, monitorizatu eta atzematea.
- **Jakinarazpenen babesa:** Jakinarazpen seguruak bermatzeko helburua duten produktuak, baimendu gabeko sarbideak edota beste sare batzuetatik datozen erasoak saihesteko. Trafikoa kontrolatu, aztertu eta horren inguruko azterketa bat egiteko.

- **Gailu mugikorren segurtasuna:** Haririk gabeko sareak eta gailu mugikorrak babestera bideratutako tresnak, segurtasun istripuak saihesteko.

Bestalde, zibersegurtasun arloko zerbitzuen kategoriari dagozkion elementuak agertzen dira; kontrola eramateko, legea betetzeko, segurtasuna kudeatzeko, istripuen jarraipena egiteko eta abar. Bakoitzaren aplikazio eremua ere zehazten da.

ZERBITZU KATEGORIA		Pertsonak	Informazioa	Azpiegitura	Negozioa
	Ikuskaritza teknikoa		☑	☑	
	Araudi ziurtagiria	☑	☑	☑	☑
	Kontingentzia eta jarraitutasuna				☑
	Legea betetzea	☑	☑	☑	
	Prestakuntza eta kontzientziazioa	☑			
	Istripuen kudeaketa	☑	☑	☑	
	Konponbideak ezartzea			☑	
	Lainoko segurtasuna		☑	☑	☑
	Euskarria eta mantentze-lana		☑	☑	

Aipatutako zerbitzuetako bakoitzerako azalpen labur bat gehitu da:

- **Ikuskaritza teknikoa:** Segurtasun arloko diagnostiko teknikoak egitera bideratutako zerbitzuak, orokorrean, estandar bat erreferentzia moduan hartuz, segurtasun egoera aztertu eta egon daitezkeen ahultasunak

edota mehatxuak atzemateko. Segurtasun arloko gertakari baten ostean ere egin daitezke, arrazoiak eta ondorioak aztertzeko.

- **Araudi ziurtagiria:** Araudia ezarri eta betetzeko erraztasunak ematera bideratutako zerbitzuak, baita araudiei dagozkien ziurtagiriak lortzeko ere.
- **Kontingentzia eta jarraitutasuna:** Zerbitzuen jarraitutasuna bermatzeko eta prozesu kritikoak babesteko helburua duten zerbitzuak, kontingentzia eta jarraitutasun planak landu eta aplikatuz. Erakundearen funtzio kritikoen jarraitutasuna bermatzeko kontingentzia eta jarraitutasun planak burutzera bideratuta.
- **Legea betetzea:** Enpresei segurtasun teknologikoaren arloko araudia betetzen laguntzeko helburua duten zerbitzuak dira.
- **Prestakuntza eta kontzientziazioa:** Informazioaren segurtasunarekin erlazionatutako prestakuntza ematera bideratutako zerbitzuak, informazioaren segurtasunaren aspektu juridiko eta teknikoen berri zabaltzeko helburuarekin.
- **Istripuen kudeaketa:** Informazioaren segurtasunarekin erlazionatutako gertakariak atzeman, saihestu eta konpontzeko zerbitzuak. Helburua sistemen ahultasunak atzeman eta identifikatzeko informazioa ematea da. Segurtasun-jarduerak kudeatzeko, gertatu aurretik, bitartean eta ostean.
- **Konponbideak ezartzea:** Erakundeetan segurtasunerako azpiegitura eta konponbide teknologikoak diseinatu, integratu eta martxan jartzera bideratutako zerbitzuak, babesteko helburuarekin.
- **Lainoko segurtasuna:** Berreskuratze-sistema edo babes politiken bidez segurtasun gertakari baten ondorioak murrizteko lainoan jarritako azpiegiturak babestera bideratutako zerbitzuak.
- **Euskarria eta mantentze-lana:** Segurtasunean espezializatutako enpresa bat beste enpresa baten mantentze, azpiegitura edo sistemez arduratzeko bidea ematen du.

Zehaztutako taxonomiaren bidez, zibersegurtasunaren barruko produktu edo zerbitzu bakoitzaren kategoria identifikatzen da, dagokion eremuan sailkatuz.