Javier Diéguez, Cyberzaintza-ko zuzendari nagusia: “Sarean lan egitea garrantzitsua da, ziberkrimenari aurre egitea eta herrialdeko azpiegitura kalteberak babestea guztion lana baita”

Cyberzaintza, Euskadiko Zibersegurtasun Agentzia, Interneta eta teknologia digitalak erabiltzeak dakartzan mehatxuei modu integral eta transbertsalean aurre egiteko Euskadi mailan sortu den erakunde publikoa da.

Agentzia Eusko Jaurlaritzaren Segurtasun Sailera atxikita dago, eta zibersegurtasunarekin lotutako arriskuei aurre egiteko behar diren tresna eta baliabide guztiak dauzka. Javier Diéguez zuzendari nagusiarekin hitz egin dugu:

Nondik dator Cyberzaintza?

Cyberzaintza Basque Cyber Security Centre (BCSC) erakundearen bilakaera naturalaren emaitza da. Erakunde horrek 2017az geroztik arrakasta handiarekin zabaldu du zibersegurtasunaren kultura Euskadin. BCSCren ereduak euskal gizartearen egungo erronkei aurre egiteko muga batzuk zituen. Horregatik, Cyberzaintzak eskumen-esparru zabalagoa dauka.

Zergatik sortu da orain?

Pertsonen arteko harremanak geroz eta digitalizatuagoak dira, bereziki transakzio ekonomikoei dagokienez, eta horrekin batera asko areagotu dira ingurune digitalean egiten diren delituak.

Datuek oso argi adierazten dute: Ertzaintzak jasotzen dituen lau salaketetatik batek ziberdelituekin du zerikusia, eta horien % 90 ziberiruzurrak dira.

Azken urtean, ziberdelituak nabarmen areagotu dira: urte honen hirugarren hiruhilekoa amaitzerako, 17.533 ziberdelitu jakinarazi ziren, 2022ko epe berdinean baino % 35 gehiago.

Bestalde, Eusko Jaurlaritzaren Prospekzio Soziologikoen Kabineteak aurten egindako inkesta baten arabera, euskal gizartearen % 70 oso kezkatuta edo nahiko kezkatuta dago ziberdelitu baten biktima izateko arriskuagatik. % 46k dio arrisku horren aurrean partzialki edo hein batean babestuta soilik sentitzen dela.

Eta mota horretako delituak geroz eta maizago gertatzea espero da. Aurrekaririk gabeko egoera baten aurrean gaude.

"Euskal herritarrek, instituzio publikoek eta enpresa-sareak zibersegurtasunaren arloko erreferentziazko erakunde publiko gisa ezagutu gaitzaten ahaleginduko gara."

Zein dira helburu nagusiak?

Cyberzaintza euskal gizartea eta, lehenik, Euskadiko administrazio publikoa zibersegurtasunaren inguruan informatzeko, sentsibilizatzeko eta trebatzeko sortu da, enpresa-sarearekin egiten genuen moduan.

Cyberzaintza Euskal Autonomia Erkidegoaren konfiantzazko kidea izango da Espainiako Gobernuaren zibersegurtasun-erakundeentzat, zehazki INCIBE (herritarrak eta enpresak) eta Centro Criptológico Nacional (administrazio publikoak) erakundeentzat. Ziberkrimenen aurkako borrokan, funtsezkoa ez ezik, ezinbestekoa da lankidetza.

Zein dira jarduketa-eremuak?

Ziberdelinkuentzia: Ertzaintzari eta erakunde judizialei ziberkrimenaren aurka borrokatzeko babesa ematea eta, lankidetza-esparru horren baitan, herrialdeko azpiegitura kalteberak babesten laguntzea.

Azpiegitura eta datu publikoen babesa: euskal sektore publikoaren azpiegitura digitalak elkarlanean babestuko ditugu, behar bezala funtzionatzen dutela bermatzeko.

Enpresen azpiegituren eta datuen babesa: sustapen ekonomikoaren arloan eskudun den Eusko Jaurlaritzako sailarekin lankidetzan.

Laburbilduz, Euskal Autonomia Erkidegoaren garapen digital segurua bultzatzen duten proiektuak eta ekintzak sustatzeko egingo dugu lan. Halaber, etengabeko kontzientziazio-kanpainak egingo ditugu.

Sarean lan egingo dugu zibersegurtasunarekin zerikusia duten askotariko erakunde eta eragile publiko nahiz pribatuekin (Ertzaintza, Osakidetza, unibertsitateak, Cybasque, etab.). Sarean lan egitea garrantzitsua da sektore honetan; beraz, Euskadiren segurtasun publikoan lan egitea, ziberkrimenari aurre egitea eta herrialdeko azpiegitura kalteberak babestea guztion lana da.

Ohiko elkarlana bi alorretan egingo da batik bat. Batetik, prebentzio-alderdietan eta, bestetik, gertakariaren ondorengo erantzunarekin lotutako alderdietan.

Bankuen sektoreak Internetaren aldeko apustua indartu du. Nola heltzen dio hain kaltebera den sektore horrek zibersegurtasunari? Zein dira mehatxu nagusiak?

Finantzen sektorea da, ikerketa guztien arabera, aktiboak babesten eskarmentu handiena duena. Sektore hori dirua eta informazioa babesten kontzentratzen da. Mehatxuen funtsa entitatearen izenean jokatzea da, eta SMS bidez egin ohi dira erasoak (smishing); dena den, telefono (vishing) edo posta elektroniko (phishing) bidez ere egiten dira batzuetan.

Delitu informatikoen arloan egiten diren iruzurren kopurua altua dela eta, lehentasuna eman diogu gai horri. Horretarako, Euskadiko biztanleek eta enpresa-sareak maiz erabiltzen dituzten entitateekin elkarlanean jarduteko bideak ezarri ditugu. Hala, gure lehen kolaboratzaileak Laboral Kutxa eta Kutxabank dira, eta haiekin elkarlanean ibili gara elkarri

“Bizum-a gure banku-entitatea bezain segurua izango da”

asmo txarreko kanpainen berri emateko eta kanpaina horiek ahalik eta bizkorren deuseztatzeko.

Bizum bidez ordaintzeko ohitura asko zabaldu da, eta zenbaitetan txartel edo transferentzia bidez ordaintzea bezain babestuta ez dagoela pentsa genezake. Berdin babestuta al dago?

Banku-entitateek eskaintzen duten banka elektronikoko aplikazioetan oinarritzen du haren babes-eskema Bizum-ek. Alegia, gure banku-entitatea bezain segurua da. Iruzurren abiapuntua berdina da beti: biktimari mezu bat bidaltzen zaio zenbateko bat bidaltzeko eskatuz. Askotan, biktimak ez daki jasotako mezua erasotzaileak dirua jasotzeko baimen-eskaera bat dela. Iruzur mota hori oso ohikoa da bigarren eskuko webguneetan. Bizum-en webgunean eraso horiei eta erreklamatzeko moduei buruzko informazio guztia agertzen da.

Internet bidezko erosketak areagotzen ari dira. Zer neurri hartzen ditugu zibererasorik ez jasateko?

Ohikoenak diren iruzurrek ezaugarri hauek dauzkate: oso eskaintza onak, klik bakarrarekin lor daitezkeen doako produktuak, beste webgune baten itxura hartzen duten sareko dendak, phishinga egiteko mezu elektronikoak eta programa edo aplikazio bat deskargatzera behartzen gaituzten mezuak.

Erosi aurretik, kontu handia eduki behar dugu onegiak diruditen eskaintzekin. Erosketaren orria fidagarria dela ziurtatu behar dugu, arakatzailearen https erreferentziari begiratu, gainontzeko pertsonen balorazioak berrikusi, etab. Gainera, ez da komeni mezu elektronikoetan jasotako esteken bidez joatea web-orri horretara, agian orri ofizialen antza duten iruzurrezko orriak baitira. Onena, arakatzailean orriaren helbidea idaztea da.

Ez da wifi-sare publikoen bidez erosketarik egin behar, eta hobe da txartel birtual bat erabiltzea, bi urratseko egiaztapenarekin. Halaber, bankuko kodeak ezin dira beste inorekin partekatu.

Erosketa egin ondoren, baimendu gabeko kargurik ez dagoela egiaztatu behar da banku-kontuan. Kontu handia eduki behar dugu bidalketa-helbidea berresteko eskatzen diguten garraio-enpresen mezu elektroniko edo SMSekin. Zalantzarik izanez gero, hobe dendarekin zuzenean egiaztatzea.

Iruzur baten biktima bazara, salaketa egin behar duzu.

Erronka nagusiak

• **Herritarrak:** biztanleak sentsibilizatu eta trebatu, inguruan dituzten arriskuez ohar daitezen eta balizko erasoen aurrean beren burua babes dezaten. Nork bere burua babestea da gakoa.

• **Administrazio publikoa:** sare bat sortzea eta konfiantzan oinarritutako harremanak eraikitzea Euskadiko administrazio-egiturarekin, ezagutzak partekatzeko eta herrialdeko azpiegitura teknologikoa indartzeko, zibermehatxuak saihesteko helburuarekin.

• **Enpresa-sarea:** enpresen prestakuntza eta garapen digital segurua ahalbidetzen lagunduko dugu, sustapen ekonomikoaren arloan eskudun den sailarekin elkarlanean, eta behar diren lankidetza-harremanak ezarriko ditugu.

“Cyberzaintza zibersegurtasunaren arloko erreferentziazko erakunde publikoa izateko ahaleginak egingo ditugu”.