Telelanaren erronka, zibermehatxuak izan arren

Azken urteotan telelanak izan duen hazkundeak, batez ere pandemiaren ondorioz, zibergaizkileen jarduera areagotu du; izan ere, urruneko lan egiteko modu horrek esposizioa areagotu duela ikusi dute, eta, beraz, delituak egiteko aukera. Euskadin azken urteetan modalitate hori nabari hazi da, 2019an %3,9 izatera iritsi zen; pandemia garaian, 2020an, %5,4ra igo zen; eta 2021ean %12ra igo da, Eustaten datuen arabera.

Hazkunde jarraitua

Ziberdelinkuentziaren hazkundea ez da bakarrik Euskadin gertatu: Espainian, horrelako delituek 287.963 kasu izan zituzten 2020an, aurreko urtean baino %32 gehiago. Datu horiek guztiek mehatxuaren garrantzia erakusten dute, nahiz eta enpresa gehienak zibersegurtasuneko neurriak aplikatzearen garrantziaz kontzientziatuta dauden. Eustatek jasotzen duen moduan, enpresa txiki eta ertainen **%88,1ek dagoeneko hartu ditu segurtasun informatikoko neurriak**, hala nola softwarearen eguneratzeak, kanpoko backupak, sarerako sarbidearen kontrola eta datuen zifratzea.

Telelanaren arriskuak

Gure ohiko lanpostuan arrisku horiek pairatzen baditugu ere, gure korporazioaren babesa dugu, eta telematikoki ez bada langileen artean zabaltzen, dagoeneko ezagunak diren hurrengo arazoak ekar ditzakete:

· **Informatika-materialean eragindako kalteak.** Zibergaizkile bat gure ekipoan sartzen denean, haren eta bertan dagoen informazioaren erabateko kontrola lortzen du, eta kalteak eragin ditzake sisteman, ekipoetan itzulezinak izan daitezkeenak, hala nola hardware eta softwarean.

· **Informazio sentikorra galtzea.**

- **Enpresaren izen ona kaltetzea.** Ospeari eragindako kalteak oso larriak dira enpresa batentzat. Informazio sentikorra lapurtzeak, adibidez, kalte konponezina eragin diezaioke enpresaren konfiantzari eta sinesgarritasunari, eta, gainera, erantzukizunak sor ditzake datuen babesari dagokionez.
- **Nortasun-lapurretak erraztea.** Informazio pertsonalaren lapurretak eta identitatea ordezkatzeak enpresa baten sisteman sartzea ahalbidetzen die zibergaizkileei, informazio sentikorra eskuratzeko edo onura ekonomikoa lortzeko.
- **Malware-erasoak jasatea.** Ekipo batean software maltzurra instalatzea datuak bahitu eta erreskate ekonomikoak lortu aurreko urratsa izaten da.

VPN sareak

Tresna horren bidez, enpresaren zerbitzarietarako sarbide segurua lortzen da, Interneten nabigatzeko, enpresa-informazioaren konfidentzialtasuna eta osotasuna gordez. Horri esker,

bide pribatu baten bidez bidera ditzakegu enpresarekiko komunikazioak. Horretan, informazioa zifratuta dago, eta egiaztapen baten bidez sar gaitezke. Horrela, hainbat helburu lortzen ditugu:

· Datuen osotasuna bermatzen dugu.

· Informazioaren konfidentzialtasuna gordeko dugu, zifratze-teknika sofistikatuei esker.

· Enpresaren barne-sarea mugarik gabe erabil dezakegu. VPN batek enpresaren informazioa bulegoan bageunde bezala eskuratzea bermatzen du.

· Hotel, aireportu eta abarretako sare publiko irekiak segurtasunez erabil ditzakegu.

Aparteko neurriak

Sare pribatu birtualez gain, beharrezkoa da gure ekipoan sartzen den informazioa kontrolatzea, batez ere kanpoko gailuen bidez, hala nola USB biltegiratze-unitateen eta beste periferiko batzuen bidez; enpresako ekipoak erabilera pertsonalerako ez erabiltzea, eta enpresako ekipoan erabiltzen ditugun aplikazioak eguneratuta mantentzea.

Aldi berean, gomendagarria da enpresak berak eta taldeak segurtasun neurri hauek ezartzea:

· **Eragile anitzeko autentifikazioa gaitu (MFA),** saio-hasierako prozesuari babes-geruza gehigarri bat eransten diona; adibidez, hatz-marka digitala edo zure telefono mugikorrera bidalitako kodea sartzea.

· **Aldizka segurtasun-kopiak egin,** adibidez, kanpoko disko gogor batean. Horrek ransonware-erasoak edo nahi gabeko datuak ezabatzea saihets dezake.

· **Enpresaren informazioa babesteko euskarriak zifratzea.** Enpresak egin beharko du lan hori, erakundearen beraren politiken arabera egin beharko bailirateke.

· **Datu sentikorrak modu seguruan ezabatzea**. Biltegiratze-gailuetako datuak berreskuratzea erabat galarazten duten bitarteko eraginkorrak honako hauek dira: dokumentu fisikoak suntsitzea eta informazioa biltegiratzeko eremu osoan gainidaztea.

BCSCn lanean dihardugu telelana ahalik eta modurik seguruenean egin dadin, eta zibersegurtasunaren kultura euskal enpresa-sarean zabaltzeko, bai enpresei bai telelangileei zuzendutako webinars zerbitzuen bidez.