Business Email Compromise Erasoak

BCSC_ALERTAK_BEC_Erasoak

www.basquecybersecurity.eus

BASQUE CYBERSECURITY CENTRE

GRUPO spri TALDEA

EUSKO JAURLARITZA
GOBIERNO VASCO
EKONOMIAREN GARAPEN ETA AZPIEGITURA SAILA
DEPARTAMENTO DE DESARROLLO ECONÓMICO E INFRAESTRUCTURAS

Iraila 2018

AURKIBIDEA

Erantzukizun-amaierari buruzko klausula

Dokumentu hau informazio eta orientazio gisa ematen da. Basque CyberSecurity Centre ez da inolaz ere dokumentuan jasotzen den informazioaren erabileraren ondorioz jasandako edo eragindako, zuzeneko edo zeharkako, ustekabeko edo aparteko erantzukizun, kalte, galera edo beste edozein kosturen erantzule solidarioak edo subsidiarioa izango.

Salmenta-debeku klausula

Salmenta edo etekin ekonomikoa lortzea guztiz debekatuta dago, hargatik eragotzi gabe dokumentuaren kopia, banaketa, difusio edo zabalkundea.

1. BASQUE CYBERSECURITY CENTRE

ZIBERSEGURTASUN EUSKAL ZENTROA (BASQUE CYBERSECURITY CENTRE, aurrerantzean BCSC) Eusko Jaurlaritzako Ekonomiaren Garapen eta Azpiegitura Sailaren mendekoa den ERALDAKETA LEHIAKORRERAKO SOZIETATEA SAn (aurrerantzean SPRI Taldea) kokatzen den ekimena da. BCSC Euskadin zibersegurtasuna eta herritarren, enpresen eta erakunde publikoen konfantza digitala garatzeko erreferentziazko entitatea da, batez ere eskualde honetako ekonomiaren sektore estrategikoentzat.

BCSC euskal gizartean zibersegurtasunaren kultura areagotzeko Eusko Jaurlaritzak duen tresna da eta zerbitzu espezializatuen eskaintzaile eta eskatzaileen arteko topagunea izatera iritsi nahi du. Horrekin berrikuntzarako aukera sortu eta enpresen arteko lehiakortasuna sustatuko luke, eta herritarrek jarduera digital seguruago bat izateko ohiturak gara ditzaten ahalbidetuko litzateke.

Bere helburuak lortzeko, zehar ekimen baten modura defnitzen da BCSC, bere sorreratik bertatik Eusko Jaurlaritzako lau sail inplikatzen dituena: lehen aipatutako Garapen eta Azpiegitura Saila, Segurtasun Saila, Gobernantza Publiko eta Autogobernu Saila eta Hezkuntza Saila.

Zentroaren jardueren artean ikerkuntza proiektuak, ekintzailetza ekimenak eta estatu nahiz nazioarte mailako beste eragile eskudun batzuekiko lankidetza koordinatuak daude. Izan ere, elkarlan estuan dihardu bere Batzorde Iraunkorreko kide diren Zientzia Teknologia eta Berrikuntzaren Euskal Sareko eragileekin.

Hortaz, BCSCren eginkizuna da euskal gizartean zibersegurtasuna sustatzea eta garatzea, Euskadiko enpresa jarduera sustatzea eta erreferentzia izango den sektore profesionala sor dadin ahalbidetzea. Testuinguru horretan eragile osagarrien artean lankidetza proiektuak gara daitezen sustatzen du berrikuntza teknologikoaren alorrean, ikerkuntzarenean, eta fabrikazio aurreratuko industriarako eta beste sektore batzuetarako transferentzia teknologikoaren alorrean.

BCSCk hainbat zerbitzu ematen ditu Gertakarien aurreko Erantzun Talde modura (aurrerantzean CSIRT, bere ingelesezko siglengatik: “Computer Security Incident Response Team”). Era berean, Euskal Autonomia Erkidegoaren eremuan lanean dihardu bere gaitasuna areagotzeko mehatxu berriak garaiz antzematen eta horiei buruzko alertak ematen, informazioaren segurtasun arloko gertakarien erantzun eta analisian, eta euskal gizartearen beharrei erantzuteko prebentzio neurrien diseinuan.

2. LABURPEN EXECUTIBOA

Business Email Compromise (BEC) erasotzaileek **120.000 euroko batez besteko galerak** eragiten dizkiete enpresei. Iruzur mota horiek ugaritu egingo direla uste da (2015etik %1.300ko hazkundea izan dute) eta **tamaina guztietako enpresei** eragiten diete dagoeneko. Aurten, Trend Micro erakundearen estimazioen arabera, sortutako galerak **8.000 milioi euro** ingurukoak izan dira.

Orokorrean, zibergaizkileen estrategia zera da, ahalik eta arrisku txikienarekin eta inbertsioaren itzulkin handienarekin onura ekonomikoa lortzea. Zentzu horretan, ondoren azalduko ditugun iruzurretan zentratzen ari dira, gero eta gehiago.

2.1. Zer da?

Business Email Compromise motako erasoek pertsona baten identitatea faltsutzen dute email bidez, beste bat engainatu eta iruzurgilearen kontrolpean dagoen kontu batera transferentzia bat egin dezan eskatzeko. Phishing motako eraso tradizionaletan ez bezala, eraso horiek **biktima bakoitzarentzako bereziki diseinatuta** daude eta posta elektroniko guztiz profesionalen itxura dute. Kasu gehienetan, zibergaizkileek enpresen azken albisteak eta langileen sare sozialak aztertzen dituzte, iruzurra ahalik eta sinesgarriena izan dadin. Pertsonalizazio maila horri esker lortzen dute **spam filtroak eta bestelako babesak gainditzea**.

Diru kopuru handiak lortzeaz gain, metodo horren bidez enpresaren inguruko informazio konfidentziala ere lortzen dute, enpresari berari ekonomikoki zein ospe aldetik kalte handia ekar liezaiokeena.

2.2. Eraso motak

Business Email Compromise iruzurra oinarrizko 4 modutan eman daiteke:

- **CEO iruzurra.** Zibergaizkileek email bat bidaltzen diote, itxuraz enpresako arduradun baten izenean, transferentziak egiteko eskumena daukan langile bati. Horren bidez, zibergaizkileen kontrolpean dagoen kontu batera fondoak bidaltzeko agindua ematen zaio.
- **Faktura faltsuaren iruzurra.** Zibergaizkileek, erabiltzaile baten kontua konprometitu ostean, postan bilatzen dute iraungitzear dagoen faktura bat, gero finantza sailarekin harremanetan jarri eta ordainketa kontua beste batengatik alda dezaten eskatzeko.
- **Abokatuaren identitatea faltsutzea.** Zibergaizkilea enpresa baten abokatu taldearen izenean aritzen da eta gatazka bat konpondu edo iraungitako faktura bat ordaintzeko transferentzia bat eskatzen du.
- **Datu lapurreta.** BEC iruzur mota hau da zuzeneko fondo transferentzia bat eskatzen ez duen bakarra. Datuak lapurtzea da xede nagusia, exekutibo baten posta elektronikoa konprometituz eta informazio konfidentziala bidaltzeko eskatuz.

2.3. Euskadiren egoera

Zibersegurtasuneko Euskal Zentroak eta **Ertzaintzaren Delitu Informatikoen Sailak** email bidezko hainbat iruzur kanpaina identifikatu dituzte berriki, euskal enpresei eraso ekonomikoak egitera bideratuak. Eremu honetako hainbat enpresa kaltetuak izan direla jakinarazi digute, beraz, oso garrantzitsua da iruzur mota honen berri izatea eta nola funtzionatzen duten eta nola prebenitu daitezkeen jakitea.

2.4. Prebentzioa

Zibererasoak prebenitu edota horiei aurre egiteko, funtsezkoa da **langileak kontzientziatzea**, ohiz kanpoko eskaerak identifikatzeko gai izan daitezen eta faktura edo bankuko kontuen xedearekin erlazionatutako aldaketak eskatzen dituzten mezuekin adi ibili daitezen. Era berean, gomendagarria da enpresek beren langileei eskatzea **transferentzia elektronikoen eskaerak beste bide batzuetatik balioztatu ditzatela**; telefonoz, esaterako, email faltsuak saihesteko. Gainera, interesgarria izango litzateke **baliabide teknikoak ezartzea**, hala nola SPF, DKIM edo DMARC delakoak, eta postara **sarbidea izateko segurtasun neurri sendoak**.