MUNDU OSOKO ENPRESEN %55EK JASAN ZUTEN GUTXIENEZ PHISHING-ERASO ARRAKASTATSU BAT 2019AN

- **Erosketa-saileko langileek dute arriskurik handiena phishing-erasoak jasateko.**
- **Ziberkrimenak etekin handiagoak ematen ditu droga- eta arma-trafikoak baino.**
- **Zibersegurtasunaren kultura ezinbestekoa da zibererasoetatik babestuago egongo den gizartea sustatzeko.**

Gaur egun enpresa askok dute lantaldean erosketa-zuzendari bat. Enpresarako produktuak eta zerbitzuak erosteko politika zehazteaz arduratzen den profesionala da. Haren jarduera beharrezkoa da negozioa ahalik eta egokien garatzeko, eta beraz, bere zeregina da enpresaren kudeaketetan gehien eragiten dutenetako bat.

Horiek horrela, berebiziko garrantzia duen soslaia da, konpainiaren negozioak aurrera jarraitzearekin zuzenean lotutakoa. Funtzio hori betetzen duen pertsonak kontziente izan behar du negozioaren jarraitutasunari eragin diezaioketen arriskuez, eta horien artean zibersegurtasunarekin zerikusia dutenez. Pertsona horrek jabetu egin behar du **zibersegurtasunari buruzko kontzientziazioa, funtsezkoa baino, nahitaezkoa dela**, okerreko praxi batek enpresaren jarduera bera gelditzea eragin bailezake. Zibergaizkileek jakin badakite kolektibo hori diru-iturri garrantzitsua izan daitekeela beraientzat, eta horregatik euren jardueraren zati handi bat profesional-talde horri zuzendutako erasoak egitean datza. Horretarako, batez ere, BEC motako (ingelesez dituzten siglengatik, Business Email Compromise) iruzurrak eta nortasuna ordezten duten erasoak baliatzen dituzte.

Phishinga, denoi eragiten digun mehatxua

Zibersegurtasun-gaietan, langileek teknologia modu desegokian erabiltzeak ekar ditzakeen arriskuez ez jabetzeak etengabeko arriskuan jartzen ditu enpresak. Hori bereziki larria da antolakundean inpaktu esanguratsua izan dezaketen sailetako profesionalen kasuan, erosketa-saila esate baterako. Enpresak neurri tekniko asko ezarri arren, nahikoa da pertsona batek erantsitako fitxategi maltzur bat exekutatzea enpresa osoa kolokan jartzeko. Hori dela eta, **erosketa-saileko langileek arrisku handiagoa dute phishing-**

info@bcsc.eus | 945 010 059

Parque Tecnológico de Álava
Albert Einstein. 46-3ª – Ed. E7 01510
Vitoria-Gasteiz

kasu bat jasateko, beste langile batzuek iritsi ezin daitezkeen enpresaren zenbait datu ezagutzen dituztelako eta horietara sarbidea dutelako.

Gehien erabiltzen diren phishing-metodoetako bat hodeian zerbitzuak eta biltegiratze-sistemak erabiltzea da, phishing-mezuei benetakoen itxura emateko. Phishingaren arriskuei buruz kontzientziazio-lana egin arren eta hari aurre egiteko jardunbide onenak izan arren, gaur egun konpainia askok aitortzen dute beren goi-mailako agintariek (zuzendari nagusiek, informaziokoek, zuzendari komertzialek, etab.) isilpeko datuak bidali zituztela mota horretako eraso bati erantzutean. Kasperskyk emandako datuen arabera, 2019ko bigarren seihilekoan **Espainia izan zen munduan phishing-eraso gehien jasan zuen seigarren herrialdea**, zerrendako lehena Grezia izanik.

State of the Phish txostenak dio zibergaizkileek, batez ere, helbide elektroniko korporatiboari egiten diotela eraso, eta nortasuna ordeztu ere egiten dutela. Txosten horren esanetan, 2019an mundu osoko enpresen %55ek jasan zuten phishing-eraso arrakastatsu bat gutxienez, %88k nortasun-ordeztea erabilitako erasoen berri eman zuten, eta %86k erasoak jasan zituzten enpresaren posta elektronikoan.

"*Niri ez zait gertatuko*" okerreko usteak gidatuta, langileen eta profesionalen **%45ek aitortzen dute errepikatutako pasahitzak erabiltzen dituztela** zerbitzu bat baino gehiagotarako, %50ek baino gehiagok ez dituzte behar bezala babesten etxeko sareak (kasu batzuetan pasahitzik ere ez dute jartzen, lana etxera eraman arren), eta **%90ek diote kontu pertsonaletarako erabiltzen dituztela enpresak emandako gailuak**. Gainera, %32k diote ez daudela ohituta sare pribatu birtualen (VPN) zerbitzuak erabiltzen.

Datu horiek ikusita, argi geratzen da **langileak biktima potentzialak direla**. Erabiltzen den metodoa ingeniaritza soziala da, beraz ezinbestekoa da arriskuei buruz kontzientzia sortzeko lana, horiek ezagutu eta aurre hartzeko gai izate aldera.

Industriak inguru arriskutsuan dihardu

Ziberkrimenarekin eta ziberdelituekin lotutako zenbakiak kezkatzeko modukoak dira. McAfeeren txosten batek dioenez, **gaur egun ziberkrimenak munduko ekonomian duen inpaktua 490.000 milioi eurokoa da**, eta zenbait kalkuluren arabera, droga- eta arma-trafikoarena baino etekin handiagoa da hori. Eraso horietako gehienak modu masiboan eta bereizketarik gabe egiten dira, eta horren ondorioz enpresa txikiei eragiten diete zuzenean; kasu askotan, ez da egoten kaltea konpontzerik. Izan ere, txostenaren datuek adierazten dute **enpresa txiki eta ertainen %60 ez direla beren onera bueltatzen zibereraso bat jasan ondoren**, eta jasan osteko sei hilabeteetan itxi egiten direla.

Azken urteetan, ziberkrimenaren negozioa profesionalizatu egin da. Egileak taldeak izaten dira, ahalik eta arriskurik txikienaz eta ahalik eta inbertsioaren zatirik handiena berreskuratuz etekin ekonomikoa lortzeko estrategia dutenak; hori dela eta, ahalik eta denbora gehienean ez nabarmentzen ahalegintzen dira.

Kalkulatu izan da 49 eta 245 egun artean igarotzen direla enpresa bat jabetu arte bere sistemak kolokan daudela, hau da, hilabete eta erdi, kalkulu baikorrenaren kasuan.

2017an, **978 milioi laguni eragin zien** ziberkrimenak, moduren batean ala bestean: iruzurrak, nortasuna ordeztea, malware-infekzioak, baimenik gabe sartzea... Kopuruak argiago adierazteko, **Europako eta Indonesiako herritar guztiak ziberkrimenaren biktima izan balira bezala da**, munduko populazioren %13 inguru. Ertzaintzaren datuen arabera, delitu informatikoekin lotuta Euskadin egindako salaketa-kopurua 9.217koa izan zen 2017an, 12.785ekoa 2018an, eta 14.311koa 2019an. Horrek erakusten du zein izan den euskal herritarrengan izandako eraginaren bilakabidea.

BCSC abian jarri zenetik une oro gizarte seguruagoa sustatzeko ahalegina egin da, eta horregatik kontzientziazio-jardunaldiak antolatzen dira hainbat publiko objektiborentzat, hala nola **IT eta OT inguruetan dabiltzan profesionalak**. Jardunaldi horietan informazioa ematen da erabiltzaileentzako arrisku ohikoenez, eta babes-neurriak ezartzea bultzatzen da. Horrek, zibermehatxuei aurre egiteko erresilientzia hobetzen laguntzeaz gain, enpresei balio erantsia emango die, jorratzen dituzten merkatuetan lehiatzeko eta berritzeko ahalmenari eusteko.

info@bcsc.eus | 945 010 059

Parque Tecnológico de Álava
Albert Einstein. 46-3ª – Ed. E7 01510
Vitoria-Gasteiz