ERAKUNDE PUBLIKOAK, INTERES HANDIKO JOMUGA ZIBERKRIMINALENTZAT

- **Sektore zibergaizkileen jomuga nagusietako bat da.**
- **Erakunde publikoei egindako erasoen arrazoia ekonomikoa izaten da kasuen %75ean.**

Gobernu-erakundeak zibergaizkileentzat jomuga interesgarria izateko arrazoiek eskaintzen duten zerbitzuaren garrantziarekin zerikusia izan ohi dute, baita iritzi publikoan mota horretako eraso batek ospearen aldetik duen inpaktuarekin ere.

Verizonek egindako Data Breach Investigations Report (DBIR) 2020 txostenean atal espezifiko bat dago, gehienbat erakunde publikoei eragiten dieten zibermehatxuei buruzkoa, eta sektore horrek duen arazo handiena web-aplikazioei egindako erasoak direla dioena. **Malware-erasoak dira ugarienak, eta haien ondoren, galdutako eta ebatsitako aktiboak**. Lehenbiziko kasuari dagokionez, malwarea pertsona batek deskargatu ohi du, edo zuzenean instalatzen du sisteman (kasuen %43an, arazo hori antolakundearen beraren barnean sortzen da), eta horrek zuzenean eragiten du segurtasun-arrakala bat.

Sektore gehienetan gertatzen den bezala, ohiko zibersegurartasun-arazo bat (%30 inguru) sistemen edo zerbitzuen okerreko konfigurazioa izaten da. Bestalde, **erasook helburu ekonomikoa izan ohi dute; horixe izaten da haien arrazoi nagusia kasuen %75etan**. Hain zuzen ere, 2019ra arte arrazoi nagusia izandakoen tokia hartu dute helburu ekonomikoek; espioitzarena. 2020ko datuen arabera behera egin du azken horren garrantziak, eta erasoen %19 baino ez dira arrazoi horrengatik egiten; **zibereraso baten ondorioz galdutako datuak pertsonalak (%51)** edo egiaztagiriei buruzkoak (%33) izaten direla ere adierazten dute datuok.

Txostenak emandako datuei gaineratu behar zaio edozein antolakunderen eguneroko jardunean **eguneratuta egotea eta teknologiaren erritmoari jarraitzea erraza ez bada, administrazio publikoan are nabarmenagoa dela hori**. Gainera, zibergaizkileek gero eta baliabide gehiago dute, espezializatuago daude, eta ez dute beren ekintzak gauzatzeko mugarik, ez prozeduraren ez moralaren aldetik; horren ondorioz, erakunde publikoentzat gero eta handiagoa da arriskua. Arazo horri berehala heldu behar zaio.

Pertsonak, sendotu beharreko katearen begia

info@bcsc.eus | 945 010 059

Arabako Teknologia Parkea
Albert Einstein. 46-3. – Ed. E7 01510
Vitoria-Gasteiz

Esan beharra dago **neurri teknikoak ezartzea bezain garrantzitsua edo are garrantzitsuagoa dela langileen kontzientzia garatzea internet eta teknologia berriak erabiltzeak dakartzan arriskuei dagokienez**. Abiapuntu gisa, kontuan izan behar dugu klik bakarrak kolokan jar dezakeela sare osoa, eta beraz haren parte diren guztiek ondo gogoan izan behar dutela zeintzuk diren hondamendi bat eragin dezaketen jarrera arduragabeak. Horregatik, langileen kontzientzia jorratu beharra dago haien lan-arloa edozein dela ere, baina kasuistikak egokituz, ulergarriak eta erabilgarriak izan daitezen eta barneratzeko eta berenganatzeko modua izan dezaten.

Edozein entitatek, eta batez ere arrisku handiagoa dutenek, sektore publikokoak kasu, kontziente izan behar du mundu honen “normaltasun berria” teknologia eta zibereraso bat jasateko etengabeko mehatxua direla, eta ondorioz jarduteko era egokitu behar duela, arriskua behar bezala kudeatzeko eta ziurgabetasunezko testuinguru honetan aritu ahal izatea ahalbidetuko dion heldutasunera iristeko.

BCSCn infografia bat prestatu dugu, **langile publikoen artean zibersegurtasun-maila hoberena sustatzeko gomendio-sorta bat emanez**. Gomendio horiek multzo hauetan sailkatuta daude: talde korporatiboa, sare sozialak, gailu mugikorrak, posta elektronikoa eta informazioa partekatzeko metodoak.

Erakunde publikoetako langileei jarduteko oinarrizko jarraibideak ematea da infografiaren helburua. Hala, arriskua gutxituko dute, bai beraientzat bai lanean ari diren entitatearentzat, jakitun izanik **denok garela gure antolakundeak zibermehatxuen aurka egiteko duen babesaren parte aktiboak.**

info@bcsc.eus | 945 010 059

Arabako Teknologia Parkea
Albert Einstein. 46-3. – Ed. E7 01510
Vitoria-Gasteiz