ZIBERSEGURTASUNEKO GERTAKARIETARAKO GOMENDIOAK

Zibersegurtasuneko gertakari baten aurrean erantzuteko beharra izanez gero, ZIURetik gomendio hauek ematen dizkizuegu:

- Horrelako gertakari baten aurrean, lehenik eta behin, haren berri eman behar zaio Ertzaintzaren Delitu Informatikoen Unitateari. Unitate horretako harremanetarako pertsona Manuel Viota jauna da. Jakinarazpena eginez gero, komeni da aipatzea ZIURetik gomendatu dela urrats hori ematea.

  Harremanetarako datuak:

  677 917 314

  di@ertzaintza.eus

- Bigarrenik, ebaluazio bat egin behar da, segurtasuneko gertakariaren ostean izaera pertsonaleko datuak galdu diren edo horien pribatutasuna arriskuan jarri ote diren jakiteko, bai eta horren berri eman behar den jakiteko.

Hala bada, eta...

- Erakunde pribatu bat bazara, segurtasun arrakala Datuak Babesteko Espainiako Agentziari jakinarazi behar zaio, gertakariaren berri izan eta 72 ordu naturaleko epean: www.aepd.es

- Euskal Autonomia Erkidegora mugatutako erakunde publikoa bazara, Datuak Babesteko Euskal Bulegoari jakinarazi behar zaio, gertakariaren berri izan eta 72 ordu naturaleko epean: www.avpd.euskadi.eus

- Jarraian dagoen gidan aurkituko duzu puntu honekin lotutako informazio gehiago.
  www.aepd.es/sites/default/files/2019-09/guia-brechas-seguridad.pdf

Jasandako gertakaria Ransomware motako software gaizto batekin lotuta badago eta gaitasun teknikoa baduzu, iturri irekiak kontsulta ditzakezu: adibidez, www.nomoreransom.org (Europolen bermea eta babesa ditu). Horietan, erraz inplementa daitezkeen neurriak aurkituko dituzu, arazoa konpontzeko eta arintzeko, baldin eta gertakaria eragin duen Ransomware familia ezagutzen bada.

Zibererasoak kudeatzeko gaitutako zentroak. Eraso bat jasanez gero, horietara jotzea gomendatzen dugu:

IZAERA PUBLIKOKO ZENTROAK:

- **BASQUE CYBER SECURITY CENTRE:**
  www.basquecybersecurity.eus/eu/

  www.basquecybersecurity.eus/eu/intzidenteei-erantzutea/

  900 104 891

  incidencias@bcsc.eus // arazoak@bcsc.eus

- **INCIBE:** www.incibe-cert.es

  www.incibe-cert.es/respuesta-incidentes

  incidencias@incibe-cert.es

IZAERA PRIBATUKO ZENTROAK:

(Gipuzkoako lurraldean dauden enpresa ziurtatuak)

- **S21sec:** IRT (Incident Response Team) bat du bere SOCean (Security Operation Center) malwarea aztertzeko eta hartu beharreko neurriak definitzeko: www.s21sec.com

- **ITS Security:** zibersegurtasuneko zerbitzu kudeatuak eta FIRST ziurtagiria duen SOC (Security Operation Center) bat ditu: www.its-security.es

- Erreferentzia gisa, ziurtatutako beste CSIRT batzuk kontsulta daitezke ENISA Sareen eta Informazioaren Segurtasunerako Europako Agentziak argitaratutako esteka honetan: www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map

T. 943 24 09 88
Zuatzu Enpresa Parkea, Urola eraikina,
2 Lokala, 1. Solairua **/ Donostia-San Sebastian**

info@ziur.eus
www.ziur.eus

@ZiurFundazioa
ZIUR Industrial Cyber Security Center

ZIURetik, gainera, aukera hau baliatu nahi dugu honako gomendio eta aholku hauek partekatzeko, zibersegurtasuneko gertakariei aurrea hartzeari eta horien aurrean babesteari buruz.

INGENIARITZA SOZIALEKO ERASOEN AURREKO PREBENTZIOA HOBETZEKO GOMENDIO OROKORRAK

Erakundeko erabiltzaileak **kontzientziatzea, sentsibilizatzea eta trebatzea**, prestakuntza horiek mehatxuen eta ahultasunen bilakaeraren arabera eguneratuz.

Posta elektroniko korporatiboan spamaren aurkako sistemak eta sandboxing sistemak erabiltzea.

Konfigurazio segurua, erabiltzaileen nabigatzaileetan **script**en blokeoa kontrolatu ahal izateko.

Erabiltzaileen **nabigatzaileak** beti eguneratuta edukitzea (Internet Explorer, Firefox, Chrome, etab.)

Internetetik deskargatutako aplikazioetan (Microsoft Word, Excel…) **makroak** automatikoki aktibatzen ez uztea

Sistema, aplikazio eta segurtasun sistema guztiak fabrikatzaileen laguntzarekin mantentzea eta **beti eguneratuta** edukitzea.

Sistema guztietan **segurtasun konfigurazio** egokiak aplikatzea:

- Beharrezkoak ez diren edo arriskutsuak izan daitezkeen funtzionalitateak desaktibatuz.
- Sistema Eragileek eskaintzen dituzten babesak erabiliz.
- Sarea segmentatuz.

Segurtasun sistema egokiak erabiltzea **mehatxuak identifikatzeko eta horiei aurre egiteko**, hala nola firewallak eta segurtasun soluzioak, end-pointean eta zerbitzari fisikoen edo birtualen sareko unitateetan.

Segurtasun kopiak maiz egitea, sistemetara etengabe edo sare segmentu berean konektatuta eduki gabe; ongi funtzionatzen dutela egiaztatzea.

Erabiltzaileei ekipoak **administratzeko baimenik ez ematea.**

Birusen aurkako soluzio bat edukitzea eta eguneratuta mantentzea.

Zibererresilientzia gaitasunak garatzea eta, gertakaririk egonez gero, informazioaren eta eragiketen teknologien **jarraitutasuna** eta **berreskurapena** ebaluatzea.

Ziberarriskuko polizen erabilera ebaluatzea, gertakaririk izanez gero, inpaktua minimizatzeko.

T. 943 24 09 88
Zuatzu Enpresa Parkea, Urola eraikina,
2 Lokala, 1. Solairua **/ Donostia-San Sebastian**

info@ziur.eus
www.ziur.eus

@ZiurFundazioa
ZIUR Industrial Cyber Security Center

ERASO BAT JASATEKO ARRISKUA MURRIZTEKO AHOLKU PRAKTIKOAK

1. IDENTIFIKATU:

- **Interneteko nabigazioa:** egiaztatu URLak, ziurtatu sartzen zaren webguneak ofizialak direla.
- **Posta Elektronikoa:** egiaztatu igorleak, ez ireki erabiltzaile susmagarrien edo ezezagunen mezuak. Ez egin klik eranskinetan edo esteketan horien jatorria ezagutzen ez baduzu.
- **Deskargak eta aplikazioak:** materialak eta software eguneraketak webgune ofizialetatik baino ez deskargatu.

2. BABESTU:

- Erabili **pasahitz sendoak** eta maiz aldatu.
- **Softwarea** eta **sistema** eragileak, beti eguneratuta.
- Eduki **antibirusa aktibatuta** eta konektatu ondo konfiguratutako firewall baten bidez.
- **Zifratu informazio** euskarriak, inoiz galtzen badituzu edo inork eskuratzen baditu, babestuta egon daitezen.
- Erabiltzaileen autentifikazio **faktore bikoitza** ezartzea oso irtenbide ona da.

3. URRUNEKO LANA EGITEN BADUZU:

- Ahal dela, sartu beti **gailu korporatiboetatik.**
- **Lainoa** aukera ona da.
- Egin **segurtasun kopiak**, etxean bazaude ere.
- Saiatu beti **komunikazio seguruak** erabiltzen; adibidez, sare pribatu birtualak.

T. 943 24 09 88
Zuatzu Enpresa Parkea, Urola eraikina,
2 Lokala, 1. Solairua **/ Donostia-San Sebastian**

info@ziur.eus
www.ziur.eus

@ZiurFundazioa
ZIUR Industrial Cyber Security Center