RANSOMWAREA, ZER DA, NOLA HEDATZEN DA ETA ERASORIK IZANEZ GERO ZER EGIN ZURE ENPRESA BABESTEKO.

Deskuidu batek zure enpresa ransomwarearen biktima bihur dezake. Berdin dio tamainak eta lan-sektoreak, nahikoa da zure erakundeko norbaitek iruzurrezko mezu bat irekitzea, webgune ezezagun batera sartzea edo infektatutako fitxategi batean klik egitea troiar bat zure ordenagailuan sartzeko eta datuak eskuratzea eragozteko. Momentu horretan zure enpresa zibergaizkile baten gatibu digitala bilakatzen da, eta, horrek, zure ekipoa eta informazioa berreskuratzeko, erreskate bat ordaintzeko eskatuko dizu.

Ransomwarea ekipo informatiko baten datuak edo sistema eragilea zifratzeko eta bahituta mantentzeko diseinatuta dagoen software maliziatasu mota da. Enpresek pairatu dezaketen eraso informatiko ohikoena da, eta, gainera, delinkuentzia informatikorako errentagarrienetako bat. Nahiz eta erakunde gehienak ez duten tankera horretako xantaiarik onartzen, oraindik badira jendaurreko erakustaldia galarazteko, bezeroen artean ospea mantentzeko edo isilpeko datuen zabalkundea saihesteko ordaintzea nahiago dutenak. Hain zuzen, Check Point aholkularitza-enpresaren txosten baten arabera, 2020an ransomwareak mundu osoko enpresei eragindako kalteak 20.000 milioi dolarrekoak izan ziren, 2019an baino %75 gehiago. Horrenbestez, Basque CiberSecurity Centre -k, hainbat zerbitzuren bitartez, ETE -ei eta enpresa handiei horrelako arazo baten aurrean babesa eskaintzen diegu.

Hurrengo lerroetan ransomware bat nola hedatzen den eta eraso baten aurrean zure enpresa babestuta mantentzeko eman beharreko pausoak [ancla] azaltzen dizkizugu. Horretaz gain, ezagutu itzazu erasoen ondorioak [ancla] eta saihesteko egin beharrekoak [ancla].

Transmisio modu nagusiak
Hauek dira ransomwarea transmititzeko modu nagusiak:

- **Posta elektronikoa.** Transmisio-metodo sinpleena da. Askotan, zibergaizkileek masiboki bidaltzen dituzte mezu elektronikoak URL lotura faltsuekin edo hainbat formatutan erantsitako fitxategi maleziatsuekin, norbaitek nahi gabe edo akats batengatik irekitzeko itxaropenarekin. Erabiltzaileak fitxategian edo estekan klik egiten duen momentuan

bertan, ransomwarearen deskarga aktibatzen da. Horrek sistema enkriptatzen du eta biktimak erreskatea ordaindu arte pasahitza baten menpe bahituta mantentzen du.

- **Sare sozialak edo berehalako mezularitza.** Sare sozialek eta berehalako mezularitzak aukera ematen diote zibergaizkileei, lotura zein fitxategi faltsuen bitartez, biktimengana masiboki eta era oso erraz batean iristen.
- **Segurtasun zuloak.** Eguneratu gabeko aplikazio eta sistema eragile batzuek ahultasunak edo segurtasun zuloak izan ditzakete. Horiek guztiak zibergaizkileentzako oso erakargarriak izan daitezke.
- ***Malvertising* edo publizitate maltzurra.** Ohiko iragarkien publizitate-espazioak erabiltzen ditu “exploits” bidezko iragarkiak txertatzeko. Programa horiek ahultasunak bilatzen dituzte kontrola eskuratzeko edo sareko datuak bereganatzeko. Ransomware-eraso asko publizitate maltzurraren bitartez hedatzen dira.
- **Deskarga automatikoak edo *Drive-by.*** Eduki maleziatsua duten eta biktimaren baimenik gabe gauzatzen diren ezkutuko deskargak dira. Kasu honetan, arriskurik larriena da infektatutako webgune bat bisitatze hutsarekin exekutatzen dela.

Zer egin eraso baten aurrean

Zure enpresa ransomwareak kutsatu badu, neurri jakin batzuk hartu behar dituzu, eta, batez ere, ez ordaindu inoiz erreskaterik. Egitenez gero, horrelako delituen sustapenean laguntzeaz gain, ez duzu arazoa bukatu denaren eta datuak berreskuratuko dituzunaren ziurtasunik izango. Hauek dira egin beharko duzuna:

1. Ekipoa saretik deskonektatu, troiatarraren hedapena mozteko.

2. Aldatu pasahitza guztiak gailu ezberdin batetik, eta, ahal dela, beste sare batean konetatuta.

3. Zifratutako fitxategiak gorde. Baliteke aurrerago fitxategiaren enkriptatzea kentzeko gai den erremintaren bat aurkitzea.

4. Salatu erasoa agintariei eta arazoa konpontzeko bilatu Basque CyberSecurity Centre zein zibersegurtasuneko beste erakunderen baten laguntza. Adibidez, Zibersegurtasun-katalogoan lagundu zaitzakeen enpresen zerrenda zabala aurkitu dezakezu.

5. Kopiak leheneratu eta garbitu kutsatutako sistema. Orduan eta azkarrako berrezarri dena, orduan eta arinago bueltatuko zara normaltasunera.

Enpresentzako ondorioak

Enpresa baten datuak bahitzeak kalte handia eragiten dio bertako funtzionamenduari. Era berean, mota guztietako galerak eragiten ditu. Datuak bahitzean, informazioa berrezarri arte, enpresaren jarduera hainbat egunetan zehar geldi daiteke.

Ransomware-eraso baten aurrean kontuan hartu beharreko beste alderdi bat datu konfidentzialak gordetzearen akatsa da. Galera horrek nahi gabe informazio pertsonalaren edo datu konfidentzialen argitaratzea ekar dezake. Era berean, kaltetutako pertsonek zein erakundeek isunak eta demandak ordaintzea eragin dezake. Eraso-mota horien biktimek ospea galde dezakete enpresa-mailan, batez ere erasoak ez baldin badio uzten enpresari bezeroarekiko dituen betebeharrak egoki betetzen.

2020tik ransomware bidezko erasoek bilakera handia izan dute. Alde batetik, beldur-maila handitzeko eta erreskatearen ordainketa behartzeko, lapurtutako informazioaren datu batzuk argitaratzen dira. Bestetik, estortzioaren kasuan, bezeroak txantaiaren alderdi garrantzitsu bat izatera pasatzen dira eta horrek egoera oso bortitz batera eramaten du enpresa.

Azken urtean zehar, inguru nazional zein internazionalean, ransomware-erasoak pairatu dituzten enpresak asko izan dira. Joan den martxoaren 9an, Estatuko enplegu Zerbitzu Publikoak (gaztelaniaz SEPE), Espainiako Enplegu Sistema Nazionala osatzen duen Lan eta Gizarte Ekonomia Ministerioari atxikitako erakunde autonomoa, Ryuk ransomwarearen erasoa jasan zuen. Ondorioz, erakundeak informazio- eta komunikazio-sistemen eskuragarritasuna denboraldi batean zehar eten behar izan zuen.

Maiatzaren 7an, ostera, ransomware-eraso batek Colonial Pipeline -ri, Estatu Batuetako oliobide habdienaren jabeari, produktu finduen hornidura etetea eragin zion eta handik egun batzuetara, Irlandako Osasun Zerbitzuak eta Toshiba teknologia enpresak ransomware-erasoak jasan zituzten.

Segurtasun neurriak

Ersao baten aurrean, prebentzio-neurri eraginkorrak hartzea ezinbestekoa da, baita egoerari aurre egiteko modurik onena ezagutzea ere:

- Softwareak eguneratuta mantendu eta nabigatzaileak eta sistema eragileak azken segurtasun-adababakiekin izan.
- Segurtasun-kopien plan eguneratua diseinatu.

- Spam eta phishing mezu guztiak antzeman eta enpresak erabiltzen ez dituen eranskinak bloketatu.
- Erakundean zibersegurtasunaren kultura zabaldu.

Ransomwarea zibersegurtasunaren arloan enpresek duten mehatxu nagusienetako bat da. Basque CyberSecurity Centre -n gizarte digital seguru baten aldeko apustua egiten dugu, eta, horregatik, funtezkoa iruditzen zaigu era guztietako erasoei aurre egiteko kontzientziazio- eta sentsibilizazio-neurriak bultzatzea. Gure web orrian, gai orotako artikuluak aurkitu ditzakezu, enpresei zein sareko erabiltzaileei bideratuta, betiere nabigatzeko modurik seguruena sustatuz.

info@bcsc.eus | 945 236 636

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

BASQUE CYBERSECURITY CENTRE
GRUPO spri TALDEA
EUSKO JAURLARITZA GOBIERNO VASCO
EKONOMARIEN GARAPEN JASANGARRITASUN ETA INGURUMEN SAILA
DEPARTAMENTO DE DESARROLLO ECONÓMICO, SOSTENIBILIAD Y MEDIO AMBIENTE