BYOD, gailu pertsonalekin eta segurtasunarekin lan egiteko joera

Azken urteetan etxeko gailu elektroniko eta informatikoek izan duten garapena eta, berrikiago, pandemiaren eraginak, BYOD (Bring Your Own Device-ren akronimoa) fenomenoa zabaldu dute enpresetan. Ohitura bihurtu da, enpresak berak eskaintzen dituen tresnak erabili beharrean, langileek euren ordenagailu eramangarriak, smartphone eta tabletak erabiltzea lan-sarera zein beste baliabide korporatibo batzuetara konektatzeko.

Zure enpresa BYOD politikak ezartzeko asmoa badu, edo praktika hori detektatu bada eta egoera erregularizatu nahi bada, eta, hala, horren inguruko informazio sentikorra babestu, ondoren ematen dizugun informazioak arriskuaren eta onuraren balantzea egiten eta zenbait gomendio jarraitzen lagunduko dizu.

BYODaren abantailak eta eragozpenak

Balantzaren alde positiboan, erabilera profesionalerako ekipo pertsonalak erabiltzeak zera dakar:

- Erakundeek nabarmen **murriztea hardwarean eta softwarean egiten duten inbertsioa**; izan ere, lan-taldeak berak eskaintzen du, telefono mugikorra, adibidez.
- **Malgutasun eta erosotasun** handiagoa lan-taldearen aldetik. Aurreko adibidearekin jarraituz, pentsa dezagun bi telefono mugikor eraman beharrean bakarra izateak duen abantaila.
- **Produktibitatea** eta eraginkortasuna handitzea, edozein unetan eta tokitan gai garrantzitsu bati erantzuteko aukera dagoelako.
- **Telelana asko errazten du**, pandemian nabarmen hazi den modalitatea izan da.

Bestalde, kontuan izan behar da:

- **Arrisku korporatiboa areagotzen zaie langileei**, gailuetan gordetako informazioa galdu, lapurtu edo helburu maltzurrekin erabil daitekeelako.
- **Malwarera gailu horien bidez sartzeko ate berri bat irekitzen da**; izan ere, erabiltzailea gailu pertsonal horrekin sare korporatibora konektatzen denean, intrusio hori enpresaren sare osoan zehar zabal dezake.
- Lan-eremuan teknologia pertsonal edo pribatua erabiltzeak dakartzan **lege-alderdiak**, informazioaren konfidentzialtasunari, erantzukizunei, lizentzien erabilerari eta abarri dagokienez. AEPDk gida bat eskaintzen du telelanean ekipoak babesteko gomendioekin.

Zalantzarik gabe, arrisku nagusiak dira gailu horiek protokolizatzea, kontrolatzea eta enpresaren zibersegurtasun azpiegituran sor daitezkeen ahulguneak identifikatzea. Halaber

horiek erabiltzeko jardunbide egokiak hedatu eta sustatzea ere. MDM (Mobile Device Management) bezalako tresna espezifiko batzuek lagundu dezakete horretan.

Mobile Device Management, kudeaketa-tresna

Mobile Device Management (MDM) tresnek sarera konektatzen diren eta baliabide korporatiboak erabiltzen dituzten gailu mugikorrak urrunetik kontrolatzen eta kudeatzen laguntzen dute. Smartphone, tableta edo ordenagailu eramangarri korporatiboen bidez egindako ekintzak administratzeko eta haien jarraipena egiteko aukera ematen du; besteak beste, aplikazioak instalatzeko baimenak, gailuen geolokalizazioa eta horiek galduz edo lapurtuz gero babestea.

Funtzionamendua erraza da; nahikoa da aplikazioa kudeatu nahi den gailuan instalatzea. Une horretatik aurrera, MDMk datu-base irisgarri bat sortzen du administratzailearentzat. Datu-base horrek malwareak edo beste edozein gorabehera detekta ditzake, haren jarduera gainbegiratu, urrutitik konfiguratu edo blokeatu, eta kudeaketa-txostenak sortu. Tresna hori erabiltzaileen gailu pertsonaletan instala daiteke eta datu pertsonalak eta korporatiboak bereiz daitezke, CCN-CERT IA-21/13 Mehatxu Txostenean azaltzen den bezala.

Zibersegurtasun gomendioak arriskuak minimizatzeko

Gaur egun ezinezkoa da gure ekipoen segurtasuna %100ean bermatzea, baina, hala ere, langileak kontzientziatu ditzakegu, arriskuak gutxitzeko zenbait gomendioren bidez:

- Enpresako segurtasun-politiketan baimenduta dauden **aplikazioak** bakarrik deskargatu, instalatu eta eguneratu. Garrantzitsua da market ofizialak erabiltzea horiek deskargatzerakoan. Gainera, ezinbestekoa da erabilera-baldintzak ongi irakurtzea gailuetan sartzeko baimenak kontrolatzeko.
- Egiaztatu erabiltzen dituzun datuak **biltegiratzeko zerbitzuak komunikazio zifratuen bidez baimenduta** daudela.
- Nahi ezta **segurtasun-kopiak** egiteak ez gaituen erasoetatik babesten, informazio garrantzitsua berehala berreskuratzen lagunduko digu, baldin eta gailua erasotzen badute eta eskuragarri ez dagoen.
- **Gailu guztiak zifratu.** Horrela informazioa baimenik gabe eskuratzea zailagoa izango da zibererasotzaileentzat.
- Gailuak galdu edo lapurtuz gero, **urruneko lokalizaziorako** tresna oso lagungarria izan daiteke, hainbat funtzio baititu; besteak beste, terminalak aurkitzea, terminala urrutitik blokeatzea, datuak urrutitik ezabatzea edo gailuaren jardueraren jarraipena egitea exekutatzen diren aplikazioak zaintzeko.
- Ahal dela, erabili komunikazio seguruak, hala nola **Sare Pribatu Birtuala** (VPN), eta ez konektatu ekipoa sare publikoetara.

Aipatutako gomendioez gain, ezinbestekoa da enpresek eta horiek osatzen dituzten pertsonek Internet erabiltzeak dakartzan mehatxuak eta ahultasunak zuzenean ezagutzea, eta teknologia modu seguruan erabiltzeko beharraz kontzientziatzea, bereziki BYOD inguruneetan.

Zibersegurtasunak erronka etengabeak ditu, eta enpresek eta enpresa-elkarteek erronka horiei aurre egin behar diete egunero. BCSCk zibersegurtasun-beharrak asetzen eta haiei erantzuten lagundu nahi die enpresei, eta, helburu hori lortzeko, zibersegurtasun-arloko sentsibilizazio- eta prestakuntza-jardunaldiak eskaintzen dizkie pertsonei, ekintzaileei, enpresei, industriari, ETEei eta enpresetako zuzendariei.

Hizpide izan dugun fenomenoa iraileko European Ciber Security Organisation (ECSO) erakundearen zibersegurtasunari buruzko kontzientziazio-egutegian sartuta dago. Ekimena zibersegurtasunarekin lotutako hainbat alderdiri buruzko informazio erabilgarria emateko sortua izan da.