Bygythiadau cynyddol i seiberddiogelwch ac uniondeb y dysgu a'r addysgu yn y DU

Gorffennaf 2021

Cyflwyniad

Dros y degawd diwethaf, mae diwydiant ar-lein eang o wasanaethau 'twyll contract' proffesiynol wedi datblygu. Yr enw sydd wedi'i fathu ar gyfer y cwmnïau hyn yw 'melinau traethodau', er bod llawer ohonyn nhw'n darparu amrywiaeth o wasanaethau eraill yn ychwanegol at ysgrifennu traethodau. Roedd gwaith ymchwil a gyhoeddwyd gan Brifysgol Abertawe ym mis Awst 2018 yn dangos bod cynifer ag un mewn saith o fyfyrwyr sydd wedi graddio'n ddiweddar ledled y byd wedi talu rhywun i wneud aseiniad ar eu rhan.

Mae camymddwyn academaidd yn fygythiad i enw da addysg uwch y DU drwy'r byd i gyd. Fodd bynnag, mae'r goblygiadau'n mynd ymhell y tu hwnt i'r sector addysg uwch. Gallai graddedigion ymuno â'r gweithlu heb y sgiliau, yr wybodaeth a'r cymhwysedd sy'n angenrheidiol, a gallai hynny gael effaith ar iechyd a diogelwch y cyhoedd. Mae cribddeiliaeth a blacmel hefyd yn dod yn fwy o fygythiad i bobl sy'n defnyddio melinau traethodau. Efallai bod data personol wedi ei storio ar-lein heb fawr ddiogelwch neu heb ei ddiogelu o gwbl, gan olygu bod cwsmeriaid yn agored i dwyll banc a dwyn hunaniaeth.[1]

Yn 2020, nododd canllawiau QAA bod melinau traethodau wedi bod yn ceisio manteisio ar y pandemig COVID-19 i dargedu myfyrwyr. Mae QAA wedi bod yn gweithio gyda phartneriaid rhyngwladol i ganfod bygythiadau sy'n datblygu ac, ym mis Ebrill 2021 hysbysodd holl sefydliadau addysg uwch y DU i roi gwybod iddyn nhw bod Asiantaeth Ansawdd a Safonau Addysg Drydyddol Awstralia (TEQSA) wedi canfod bygythiad newydd i seiberddiogelwch.

Canfu gwaith ymchwil TEQSA bod melinau traethodau wedi bod yn cyfaddawdu gwefannau darparwyr addysg uwch yn Awstralia drwy osod cod maleisus sy'n ailgyfeirio myfyrwyr at wefannau twyll contract. Argymhellir bod darparwyr yn gwneud ymchwiliad o'u gwefannau i ganfod a ydyn nhw'n agored i gael eu camddefnyddio neu eu cyfaddawdu, a diben y ddogfen hon yw rhoi canllawiau ymarferol y gall sefydliadau eu dilyn i fynd i'r afael â'r bygythiadau hyn i seiberddiogelwch ynghyd â bygythiadau eraill.

[1] Sutherland-Smith, W a Dullaghan, K (2019), 'You don't always get what you pay for: User experiences of engaging with contract cheating sites', yn y cyfnodolyn 'Assessment & Evaluation in Higher Education', 44:8, 1148-1162, cyfeirnod DOI yr adnodd digidol: 10.1080/02602938.2019.1576028

Cyngor gan y Cydbwyllgor Systemau Gwybodaeth (Jisc) ynglŷn â sut i ymdrin â bygythiadau sy'n datblygu i seiberddiogelwch

Yn ogystal â newidiadau sylweddol yn nhactegau'r bobl sy'n defnyddio meddalwedd wystlo i dargedu sefydliadau, mae tystiolaeth gynyddol hefyd bod newid yn digwydd yn y gweithgareddau troseddol sy'n targedu myfyrwyr mewn perthynas â gwasanaethau melinau traethodau. Mae hyn yn digwydd i gefnogi economi sy'n tyfu drwy'r byd i gyd mewn gwerthu a phrynu traethodau a deunyddiau sy'n berthnasol i gyrsiau. Er nad yw hi'n anghyfreithlon i werthu neu brynu deunyddiau o'r fath yn y DU ar hyn o bryd, mae'n dwyllodrus hawlio mai eich deunyddiau chi eich hun yw'r rhain er mwyn ennill cymhwyster academaidd ffurfiol.

Yn debyg i'r tactegau gyda'r meddalwedd wystlo, y man cychwyn ar gyfer y gweithredoedd hyn yw cael mynediad heb awdurdod i systemau cyfrifiadurol. Mae ymosodiad gyda meddalwedd wystlo'n ceisio tynnu data allan, amgryptio ac analluogi seilwaith digidol gyda'r bwriad o roi sefydliad o dan y pwysau mwyaf i dalu pridwerth. Yn y mathau newydd hyn o ymosodiadau, mae troseddwyr yn ceisio herwgipio gwefannau dilys i fyfyrwyr i hyrwyddo gwasanaethau melinau traethodau drwy nifer o dactegau yn cynnwys ailgyfeirio'r defnyddiwr.

Mathau o god cyfrifiadurol maleisus

Canfu TEQSA bedwar math allweddol o god maleisus ym mharthau gwe prifysgolion yn Awstralia:

- darnau o god a osodir yng ngwefan y darparwr i ailgyfeirio myfyrwyr at wefan gwasanaeth twyllo drwy ddolen URL benodol
- dolenni at wefannau twyll contract sy'n cael eu hymwreiddio yng ngwefan y darparwr
- sylwadau a osodir i ledaenu neu ddarparu dolenni at wasanaethau twyll contract ar wefannau fforymau trafod (yn enwedig y rheiny a grëir ar sail WordPress)
- cystadlaethau traethawd/ysgoloriaeth ffug a osodir i mewn i wefannau'r darparwr, gyda'r bwriad o gasglu gwaith go iawn myfyrwyr er mwyn i'r cwmnïau twyll academaidd masnachol eu gwerthu ymlaen.

Mae'r canllawiau cyfredol gan Jisc a Chanolfan Seiberddiogelwch Genedlaethol y DU (NCSC) ynglŷn â sut i amddiffyn rhag ymosodiadau gyda meddalwedd wystlo yr un mor berthnasol i leihau effeithiau'r ymosodiadau newydd hyn. Ond, er bod meddalwedd wystlo'n ceisio bod yn hynod aflonyddgar, mae'r ymosodwyr hyn yn ceisio aros heb eu canfod ac yn barhaus cyn hired ag y gallant. Mae hyn yn golygu bod angen i staff a myfyrwyr fod yn hynod ymwybodol ac effro er mwyn eu canfod a lleihau eu heffaith mor fuan ag y bo modd.

Mae Jisc yn darparu gwasanaethau seiberddiogelwch sy'n gallu rhwystro cynnwys maleisus hysbys mewn gwefannau sy'n cynnal meddalwedd rheoli a gorchymyn neu faleiswedd hysbys, gan helpu i leihau gwe-rwydo a mathau eraill o ymosodiadau ar sector addysg ac ymchwil y DU. Darperir hyn i aelodau drwy wasanaeth datrys enw parth y rhwydwaith Janet (JNRS) lle gall yr aelod ddewis optio i mewn. Mae Jisc wrthi'n ymgynghori ar newidiadau i Bolisi Diogelwch y rhwydwaith Janet i ddarparu rhai gwasanaethau lle mae gofyn i'r aelod optio allan os nad yw eu heisiau.

Wrth geisio mynd ati'n rhagweithiol i atal y bygythiadau hyn sy'n datblygu, bydd Jisc yn gweithio gyda phrifysgolion, colegau, cyrff cynrychioli a chyrff rheoleiddio i helpu i gydlynu dull ar sail polisi o rwystro amrediad ehangach o fygythiadau i seiberddiogelwch.

Canllawiau ymarferol ac adnoddau defnyddiol

Mae'n rhaid i bob ysgol a phob coleg gadw llygad craff ar y dirwedd hon o fygythiadau sy'n datblygu. Mae nifer o'r trefnau rheoli y mae modd eu defnyddio i helpu i gryfhau seibergadernid mewn perthynas ag un o'r bygythiadau mwyaf ar hyn o bryd - meddalwedd wystlo - yn darparu buddion diogelu ehangach hefyd i ddefnyddwyr a sefydliadau. Mae hyn yn bwysig am fod myfyrwyr yn darged parhaol i seiberdroseddwyr.

Mae myfyrwyr wedi bod yn darged ers tro byd mewn twyll taliadau benthyciad myfyrwyr drwy ymosodiadau gwe-rwydo, ond mae bygythiadau cynyddol gan wasanaethau a werthir i fyfyrwyr, yn cynnwys gwefannau twyll contract neu felinau traethodau. Mae angen i fyfyrwyr fod yn ymwybodol o'r risg uwch y maent yn ei wynebu drwy ddefnyddio gwasanaethau twyll contract. Mae canllawiau QAA 'Contracting to Cheat' yn cynnwys astudiaethau achos ynglŷn â sut i hybu ymwybyddiaeth ymysg myfyrwyr.

Yn ogystal â hybu ymwybyddiaeth, dylai sefydliadau weithredu trefnau diogelu effeithiol rhag herwgipio a difwyno gwefannau, yn ogystal â'r bygythiad parhaus gan feddalwedd wystlo. Mae'r rhain yn cynnwys:

- sicrhau pob gwasanaeth drwy ddefnyddio cyfrineiriau cryf a phrofion dilysu aml-ffactor
- cynnal polisïau rheoli gwendid a chyweirio effeithiol
- cadw'n effro ac yn ymwybodol o'r ffaith bod troseddwyr yn ceisio cyfreithloni eu gwasanaethau drwy osod cynnwys yn y systemau y mae myfyrwyr yn eu defnyddio.

Os bydd coleg neu brifysgol yn dioddef ymosodiad seiber, mae trefnau adfer cymeradwy i'w dilyn. Mae'r rhain yn cynnwys:

- adfer y systemau'n effeithiol a phrydlon o gopïau wrth gefn nad ydynt ar-lein
- arfer ac ymarfer eich cynllun ymateb i ddigwyddiad ar gyfer gwahanol fathau o achosion o dorri seiberddiogelwch.

Dylai pob aelod Jisc sydd angen cymorth i atal toriadau seiberddiogelwch neu i adfer eu systemau ar ôl ymosodiadau gysylltu â thîm ymateb i ddigwyddiadau diogelwch cyfrifiadurol (CSIRT) y rhwydwaith Janet drwy e-bostio irt@csirt.ja.net neu ffonio 0300 999 2340.