

CYNGOR SIR YNYS MÔN / ISLE OF ANGLESEY COUNTY COUNCIL

Cyfarfod:	Pwyllgor Llywodraethu ac Archwilio
Dyddiad:	8 Chwefror 2024
Teitl yr Adroddiad:	Adroddiad gan y Swyddog Diogelu Data Ysgolion ar Ganlyniad Ymchwiliad Swyddfa'r Comisiynydd Gwybodaeth i'r Digwyddiad Seiber ym Mehefin 2021
Pwrpas yr Adroddiad:	Hysbysu aelodau o ganlyniad yr ymchwiliad a gwblhawyd gan yr ICO yn dilyn adrodd ar ddigwyddiad seiber a effeithiodd ar yr ysgolion uwchradd.
Pennaeth Gwasanaeth:	Marc Berw Hughes Cyfarwyddwr Addysg, Sgiliau a Phobl Ifanc MarcHughes@ynysmon.llyw.cymru
Awdur yr Adroddiad:	Elin Williams Swyddog Diogelu Data Ysgolion dpoysgolionmon@ynysmon.llyw.cymru

Pwrpas yr adroddiad hwn

Darparu trosolwg i'r Pwyllgor Llywodraethu ac Archwilio o ganlyniad i ymchwiliad Swyddfa'r Comisiynydd Gwybodaeth (ICO) i ddigwyddiad seiber yn yr ysgolion uwchradd yn 2021.

Mae'r adroddiad hefyd yn darparu trosolwg o ba weithredoedd sydd wedi eu cymryd gan y Swyddog Diogelu Data Ysgolion a Gwasanaeth TGCh y Cyngor parthed llunio rhaglen waith fewnol er mwyn cyfarch elfennau technegol a llywodraethu gwybodaeth amrywiol oedd yn ddiffygiol.

Argymhellion

Mae'r Swyddog Diogelu Data Ysgolion yn gwneud yr argymhellion canlynol i'r Pwyllgor, bod:

- i. adroddiad y Swyddog Diogelu Data Ysgolion, sy'n darparu trosolwg o ganlyniad ymchwiliad yr ICO i'r digwyddiad, yn cael ei dderbyn.
- ii. gweithredoedd sydd wedi eu hadnabod a'u cwblhau drwy'r rhaglen waith fewnol yn cael eu derbyn.

Adroddiad gan y Swyddog Diogelu Data Ysgolion ar Ganlyniad Ymchwiliad y Swyddfa'r Comisiynydd Gwybodaeth i'r Digwyddiad Seiber ym Mehefin 2021

1. Cefndir

Darganfuwyd ar y 23^{ain} o Fehefin 2021 bod achos posib o seiber-ddigwyddiad wedi bod, yn effeithio ar bob un o'r pum ysgol uwchradd sydd ar Ynys Môn - Ysgol Syr Thomas Jones; Ysgol Uwchradd Bodedern; Ysgol Gyfun Llangefni; Ysgol David Hughes ac Ysgol Uwchradd Caergybi.

Nid oedd yn hysbys ar y pryd a allai data personol a gedwir ar systemau'r ysgolion fod wedi'i beryglu yn ystod y digwyddiad. Codwyd y larwm ar ôl darganfod traffig amheus ar weinyddion e-bost ysgolion uwchradd.

Roedd systemau technoleg gwybodaeth - gan gynnwys cyfrifon e-bost - wedi cael eu hanalluogi dros dro i gyfyngu'r digwyddiad ar y pryd. Roedd tarfu ar yr ysgolion tra bod y digwyddiad yn cael ei gyfyngu.

Daeth y Cyngor â thîm o ymgynghorwyr seiber-dechnoleg arbenigol i mewn ar unwaith i ymchwilio i'r digwyddiad. Roedd y National Cyber Security Centre (NCSC) hefyd yn rhoi cymorth i ddatrys materion. Ni chanfu dadansoddiad fforensig o'r digwyddiad seiber unrhyw dystiolaeth bod systemau TGCh wedi'u hymdreiddio neu eu peryglu.

Adroddwyd ar y digwyddiad i Swyddfa'r Comisiynydd Gwybodaeth (ICO) oherwydd y risg posibl i'r cofnodion sensitif iawn a gadwir gan yr ysgolion.

2. Gweithredoedd wedi eu Cwblhau fel Rhan o'r Rhaglen Waith Fewnol yn dilyn Digwyddiad Seiber Ysgolion Uwchradd

2.1. Trosolwg

Yn dilyn y digwyddiad ym Mehefin 2021, ffurfiwyd rhaglen waith fewnol a oedd yn cynnwys nifer o gamau adfer pwysig pellgyrhaeddol er mwyn cyfarch elfennau technegol a llywodraethu gwybodaeth amrywiol oedd yn ddiffygiol.

Mae gwelliannau technegol a llywodraethu gwybodaeth wedi eu harwain gan y Swyddog Diogelu Data Ysgolion a swyddogion Gwasanaeth TGCh y Cyngor.

Mae nifer o weithredoedd pwysig wedi eu cyflawni ers i'r rhaglen gael ei gweithredu, gan gynnwys derbyn prif bolisiau diogelu data ac uwchraddio systemau ac isadeiledd technoleg gwybodaeth ysgolion.

Ysgogodd y digwyddiad y Cyngor i gyflwyno gwaith a oedd wedi'i gynllunio, fel rhan o raglen HWB Llywodraeth Cymru, i uwchraddio systemau technoleg gwybodaeth yr

ysgolion uwchradd, arbennig a chynradd. Dechreuodd y gwaith o uwchraddio'r systemau a'r seilwaith TGCh dros wyliau'r haf 2021.

Mae systemau data yr oedd yr ysgolion yn eu defnyddio wedi'u trosglwyddo i wasanaethau cwmwl HWB. Mae bod ar HWB yn helpu i wneud y systemau yn yr ysgolion mor gadarn â phosibl ac yn lleihau'r risg o unrhyw ymosodiad neu ddigwyddiad posibl yn y dyfodol.

Mae gwaith wedi'i wneud i alluogi Dilysu Aml-factor (MFA) ar gyfrifon HWB staff a llywodraethwyr ysgol i wella diogelwch wrth gyrchu HWB o gartref.

Fel rhan o'r ymateb i'r digwyddiad, penderfynwyd symud offer a ddefnyddiwyd gan ysgolion i Microsoft InTune, unwaith eto i wella diogelwch mynediad. Mae'r mudiad eisoes wedi ei gwblhau ar gyfer yr ysgolion cynradd a Canolfan Addysg y Bont, a gwaith wedi cychwyn i fudo ysgolion uwchradd.

2.2. Gwelliannau Llywodraethiant Diogelu Data

Rhif	Gweithredoedd a Gwelliannau	Cynnydd ers Gorffennaf 2021
1	Diweddarau polisïau diogelu data cyfredol a chreu polisïau newydd.	<p>Mae cyfanswm o 14 polisi diogelu data ar gyfer ysgolion wedi naill ai cael eu diweddarau'n dilyn mabwysiadu <i>UK GDPR</i> neu eu creu fel polisïau newydd:</p> <ul style="list-style-type: none"> • Polisi Diogelu Data Ysgolion • Polisi Digwyddiadau Diogelwch Data Ysgolion • Polisi Diogelwch Gwybodaeth Ysgolion • Gweithdrefn Rhannu Gwybodaeth gydag Awdurdodau Heddlu'r Deyrnas Unedig (Gwynedd a Môn) • Polisi Cais gan Wrthrych y Data Ysgolion • Polisi Prosesu Data Ysgolion • Polisi Trosglwyddo Cofnodion Ysgol i Archifdy Ynys Môn • Polisi Asesiad Effaith Diogelu Data Ysgolion • Polisi CCTV Ysgolion • Polisi Rheoli Cofnodion Ysgolion • Polisi E-Ddiogelwch Ysgolion • Polisi E-bost Staff Ysgolion • Polisi Cyfryngau Cymdeithasol Staff Ysgolion • Polisi Tynnu Lluniau at Bwrpas Cyhoedduswydd Ysgolion.

		Mae dogfen Rhestr Wirio Polisiâu Diogelu Data wedi ei ddatblygu er mwyn cefnogi ysgolion i gadarnhau eu bod wedi gweithredu ar y prif ofynion oddi fewn i'r holl bolisiau diogelu data.
2	Sicrhau bod staff a llywodraethwyr ysgolion wedi derbyn hyfforddiant diogelu data a'u bod yn ymwybodol o'u cyfrifoldebau o ran cydymffurfiaeth diogelu data.	Mae sesiynau hyfforddiant wedi eu cynnal gyda phenaethiaid, staff ysgolion a llywodraethwyr. Mae cyfanswm o 51 sesiwn hyfforddiant wedi eu cynnal rhwng Gorffennaf 2021 a Thachwedd 2023 ac mae 25 corff llywodraethol wedi bod yn gynulleidfa i gyflwyniad diogelu data.
3	Defnyddio'r Adolygiad Rheolaeth Ysgol (ARhY) i fonitro cydymffurfiaeth ac i gadarnhau pa bolisiau sydd wedi eu mabwysiadu gan ysgolion.	Defnyddir yr Adolygiad Rheolaeth Ysgol i gael gwybodaeth gwaelodlin parthed cydymffurfiaeth ac ar gyfer monitro pa ysgolion sydd wedi mabwysiadu pa bolisiau diogelu data.
4	Creu Cytundeb Lefel Gwasanaeth rhwng ysgolion a'r Cyngor ar gyfer gwasanaeth y Swyddog Diogelu Data Ysgolion.	Cafodd Cytundeb Lefel Gwasanaeth ei greu a'i rannu gydag ysgolion i'w arwyddo ym mis Tachwedd 2021 yn dilyn cyfnod o ymgynghori. Mae'r CLG cyfredol yn cael ei adolygu ym mis Mawrth 2024.
5	Mapio'r llifiau data rhwng yr ysgolion a'r Cyngor.	Sefydlwyd grŵp i edrych ar gytundebau a phrosesau sydd yn eu lle rhwng ysgolion a'r Cyngor er mwyn adnabod ble mae angen cytundeb. Mae gwaith yn parhau gyda'r ffrwd gwaith hwn.
6	Adolygu trefniadau gyda phroseswyr data a chreu/adolygu Cytundebau Prosesu Data lle bo angen.	Mae gwaith mapio o gwmpas pa systemau, rhaglenni ac apiau mae pob ysgol unigol yn eu defnyddio wedi ei gwblhau. Mae hyn wedi dangos a oes gan ysgolion Gytundebau Prosesu Data addas eisoes ar waith ac mae gwaith pellach wedi ei gwblhau er mwyn creu Cytundebau Prosesu Data newydd lle bo angen a phan fo apiau a rhaglenni newydd yn cael eu defnyddio. Mae gwaith yn parhau gyda'r ffrwd gwaith hwn.
7	Creu Pecyn Cofnodion Gweithgareddau Prosesu (ROPA) a Phecyn Cofrestr Asedau Gwybodaeth.	Datblygwyd canllaw ar sut i greu ROPA. Yn lle darparu templed i ysgolion ei gwblhau eu hunain, mae'r Swyddog Diogelu Data Ysgolion wedi bod yn datblygu templed ROPA sydd wedi ei boblogi'n barod i ysgolion ei addasu (fersiwn ar gyfer y cynradd a'r uwchradd). Mae hyn hefyd yn cynnwys Cofrestr Asedau Gwybodaeth. Mae'r rhain wedi eu datblygu'n defnyddio gwybodaeth

		wedi ei chasglu o'r gwaith mapio ynglŷn â pha systemau, rhaglenni ac apiau sy'n cael eu defnyddio. Mae'r templedi yn barod i'w cymeradwyo a bydd sesiynau'n cael eu cynnal er mwyn cefnogi ysgolion gydag addasu'r templedi.
8	Creu Pecyn Asesiad Effaith Diogelu Data Ysgolion (DPIA).	Mae templed Rhestr Risg a Matrics Risg wedi eu datblygu ac wedi eu rhannu gydag ysgolion er mwyn cefnogi ysgolion unigol i adnabod a monitro risgiau diogelu data.
9	Cwblhau Asesiadau Effaith Diogelu Data (DPIA).	Mae templed DPIA cyffredinol wedi ei greu i ysgolion perthnasol ei addasu ar gyfer eu system CCTV. Mae gwaith yn parhau gyda'r ffrwd gwaith hwn.
10	Creu pecyn ffurflen ganiatâd.	Mae'r ffurflen ganiatâd gyfredol ar gyfer cyhoeddi lluniau ar amrywiaeth o lwyfannau wedi ei hadolygu a'i diweddarau ac mae taflen wedi ei chynhyrchu er mwyn egluro i ddisgyblion a rhieni sut mae caniatâd <i>UK GDPR</i> yn gweithio.
11	Cynnal archwiliad diogelu data.	Mae'r Swyddog Diogelu Data Ysgolion wedi ymweld â phob ysgol unigol er mwyn adolygu cydymffurfiaeth a threfniadau diogelu data yn 2022 a 2023.
12	Trafod materion diogelu data ysgolion gyda'r Fforwm Cynradd a'r Fforwm Uwchradd a rhannu'r newyddlen diweddariad diogelu data ysgolion.	Mae'r Swyddog Diogelu Data Ysgolion yn paratoi diweddariadau rheolaidd i ysgolion, sy'n cynnwys rhannu newyddlen dymhorol. Mae rhan diogelu data ysgolion yn y bwletin llywodraethwyr ysgol hefyd ac mae diweddariadau a gwybodaeth ynglŷn â diogelu data yn cael eu darparu'n rheolaidd drwy fwletin wythnosol y Gwasanaeth Dysgu. Mae'r Swyddog Diogelu Data Ysgolion yn cael gwahoddiad yn rheolaidd i fynychu cyfarfodydd Fforwm Strategol Cynradd a Fforwm Strategol Uwchradd a hefyd yn aelod o'r Fforwm TGCh Ysgolion a'r Gweithgor Gwella Systemau a Phrosesau. Mae tudalen diogelu data ar feicrowefan y Gwasanaeth Dysgu ble mae holl bolisïau, canllawiau a thempledi cyfredol ar gael i ysgolion eu defnyddio, ac mae Grŵp Gweithredol Diogelu Data Ysgolion wedi ei sefydlu.

2.3. Gwelliannau TGCh

Mae'r canlynol yn welliannau sydd wedi eu hargymell gan y cwmni a gefnogodd Cyngor Sir Ynys Môn yn dilyn y digwyddiad seiber ysgolion uwchradd (Grŵp NCC).

Rhif	Gwelliannau yr Argymhellir	Cynnydd hyd yma
1	Uwchraddio systemau gweithredu etifeddiaeth	Drwy fudo i InTune, mae fersiynau cyfredol o Windows wedi eu gosod neu mae'r cyfrifiadur wedi ei ddad-gomisiynu os nad oedd diweddarau yn bosib.
2	Gweithredu Dilysu Aml-Factor (MFA)	Mae MFA yn ei le drwy InTune. Mae unrhyw geisiadau i fewngofnodi o du allan i rwydwaith yr ysgol angen MFA.
3	Analluogi protocolau etifeddiaeth e-bost (IMAP & POP3)	Hyn wedi ei gyfarch drwy'r defnydd o system e-bost HWB.
4	Diweddarau sgan gwrthfyrssau	Mae'r holl offer sydd wedi mudo i InTune yn derbyn diweddariadau Defender.
5	Datrysiad cyfrinair gweinyddwr lleol Microsoft	Mae offer yn cael cyfrifon gweinyddol sy'n unigryw ac yn gymhleth. Mae manylion yn cael eu cadw'n ddiogel gan y tîm TGCh.
6	<i>Remote desktop hardening</i>	Mae <i>remote desktop</i> wedi ei analluogi.
7	Cyfyngu mynediad i'r we	Mae mynediad i'r we wedi ei analluogi o <i>servers</i> .
8	Galluogi <i>Endpoint Detection and Response (EDR)</i>	Angen paratoi achos busnes pan mae mudiad ysgolion uwchradd wedi ei gwblhau.
9	<i>SIEM solution</i>	Mae SIEM wedi ei osod yn gorfforaethol, ac mae gwaith wedi ei gychwyn i edrych ar fewnforio data ysgolion.
10	Breintiau cyfrifon	Nid yw cyfrifon ar offer yn gyfrifon gweinyddwyr.
11	Adolygu rheolaeth <i>patch</i>	Mae diweddariadau'n cael eu rheoli drwy osodiadau InTune ac mae'r tîm isadeiledd yn trefnu diweddariadau ar gyfer pecynnau eraill fel bo angen.
12	Adolygu rhaglenni sydd o bosibl yn ddiangen	Mae pob cyfrifiadur wedi ei ail-ffurfweddu a dim ond meddalwedd sydd wedi ei gymeradwyo sy'n cael ei osod.

3. Canlyniad i Ymchwiliad Swyddfa'r Comisiynydd Gwybodaeth

Mae'r ICO wedi rhannu eu canlyniad i'w hymchwiliad drwy lythyr yn Ebrill 2023, yn dilyn y Cyngor yn adrodd am y digwyddiad iddynt ym Mehefin 2021. Bu i'r ICO gadarnhau bod y digwyddiad wedi ei ystyried o dan Reoliad Diogelu Data Cyffredinol y Deyrnas Unedig (RhDDC y DU) oherwydd natur y prosesu yn ymwneud â hyn ac nad oes angen ymyrraeth bellach ganddynt.

Yn ystod ymchwiliadau i'r digwyddiad, bu i'r ICO ddarganfod bod amryw o elfennau technegol a llywodraethu gwybodaeth sy'n angenrheidiol i gydymffurfio â'r ddeddfwriaeth berthnasol yn ddifffygiol. Amlygwyd y diffygion technegol mewn adroddiad

gan yr NCSC (National Cyber Security Centre), arbenigwyr pennaf y DU ar ddiogelwch seiber.

Yn ogystal â hyn, mae'r ICO yn cynnig anogaeth i barhau gyda'r gwelliannau technegol a llywodraethiant diogelu data yn yr ysgolion.

4. Casgliadau

Mae'n amlwg bod gallu'r Cyngor i adnabod a nodi beth oedd angen ei fabwysiadu â'i wella yn dderbyniol i'r ICO, a bod hyn wedi atal ymyrraeth bellach

Mae'r Swyddog Diogelu Data Ysgolion a swyddogion Gwasanaeth TGCh y Cyngor wedi parhau gyda'r gwelliannau technegol a llywodraethu diogelu data yn yr ysgolion, fel yr argymhellir gan yr ICO.

Mae parhau gyda'r rhaglen waith yn hanfodol bwysig er mwyn creu isadeiledd digidol diogel a diwylliant cryf o amddiffyn data yn ein hysgolion. Bydd y Swyddog Diogelu Data Ysgolion a Gwasanaeth TGCh y Cyngor yn parhau i gefnogi ysgolion er mwyn cwblhau'r rhaglen waith a sicrhau bod gan bob ysgol y polisïau, y dogfennau allweddol, yr ymarferion gorau a'r dechnoleg briodol er mwyn cydymffurfio'n llawn â gofynion diogelu data.

Mae ymosodiadau seiber yn dal i fod yn fygythiad gwirioneddol i ysgolion, ond mae'r gwaith o uwchraddio'r systemau a'r seilwaith, ynghyd ag ymarferion cydymffurfio diogelu data da, yn rhoi ysgolion mewn sefyllfa fwy diogel wrth fynd ymlaen.