CYFARFOD: **PWYLLGOR ARCHWILIO A LLYWODRAETHU**

DYDDIAD: **15 GORFFENNAF 2021**

TEITL: **GWYDNWCH SYSTEMAU T.G. - DIOGELWCH SEIBR**

PWRPAS: **Diweddaru'r Pwyllgor am wytnwch diogelwch seibr Cyngor Gwynedd, a rhoi cyfle i'r aelodau graffu'r sefyllfa. Bu sôn am ymosodiadau seibr yn y newyddion yn ddiweddar, a gyda chynnydd yn ein dibyniaeth a defnydd o dechnoleg, mae'n amserol i adrodd ar yr hyn sy'n digwydd yn lleol yn y Cyngor.**

AWDUR: **HUW YNYR, PENNAETH CYNORTHWYOL CYLLID – TECHNOLEG GWYBODAETH**

AELOD CABINET: **CYNGHORYDD IOAN THOMAS**

---

1. Crynodeb

1.1 Mae'r Cyngor â dyletswydd i ddarparu amrywiaeth eang o wasanaethau, nifer ohonynt yn defnyddio adnoddau technolegol. Mae'n hanfodol i sicrhau fod yr amgylchedd hwnnw wedi'i ddiogelu rhag bygythiadau fyddai'n medru tanseilio gallu'r Cyngor i ddarparu gwasanaethau ac yn peryglu data yng ngofal y Cyngor.

1.2 Mae'r adroddiad hon fod er gwybodaeth yn unig, gan lunio darlun lleygwr o'r ddarpariaeth diogelwch seibr sydd wedi ei baratoi gan y Gwasanaeth Technoleg Gwybodaeth. Nodir bod darpariaeth mewn lle i liniaru'r risg o ymosodiad seibr, ond ni ellir gwarantu 100% na fyddai modd i ymosodiad dorri trwy ein amddiffynfeydd. Mae'r gosodiad yma'n wir am bob sefydliad, ond mae mesurau pellach yn eu lle i adfer ein systemau pe byddai ymosodiad yn torri drwy ein amddiffynfeydd.

1.3 Er bod pwyslais i weld yn y cyfryngau ar ddiogelwch seibr, mewn gwirionedd, fe ddylai'r pwyslais fod ar wytnwch seibr, sy'n cynnwys yr elfennau o ddiogelu drwy adeiladu amddiffynfeydd, ond hefyd yn cynnwys y gallu i adfer ein hunain o sefyllfa bregus pe byddai'r amddiffynfeydd hynny'n methu.

2. Cefndir

2.1 Rydym yn ymwybodol bod ymgyrchwyr yn y maes yn chwilio am wendid yn amddiffynfeydd cyrff cyhoeddus. Felly, byddai'n amhriodol cymryd safbwynt na fyddai'r Cyngor yn darged tebygol i'r sawl sydd yn cynnal ymosodiadau seibr, er gallai corff cyhoeddus cymharol fychan heb warchodfeydd effeithiol fod yn darged haws ar gyfer seibr derfysgaeth.

2.2 Gan fod hwn yn faes byw, mae'r ymosodiadau'n esblygu drwy'r amser a mae'n dipyn o sialens i gadw amgylchedd yn gyfredol i gynnal gwasanaethau gwydn. Mae safon y mesurau diogelwch yn ddibynnol ar ystod eang o ffactorau, h.y. mesurau technolegol, ffisegol a gweinyddol, ac mae gan bob unigolyn o fewn y Cyngor a'i bartneriaid rôl hanfodol i'w chwarae rhag eu tanseilio.

2.3 Mae'r Cyngor yn dwyn ar amryw o ffynonellau i ddatblygu a chynnal amgylchedd gwydn, gan gynnwys:

- Safonau ac ymarfer da yn y maes sy'n cael eu cyhoeddi gan gorff cynghori Llywodraeth y Deyrnas Unedig ar eitemau seibr, yr NCSC (*National Cyber Security Centre*);
- Aelodaeth â chyrff sy'n rhybuddio am ddigwyddiadau a gwendidau fel y gallwn ymateb yn brydlon;
- Buddsoddi mewn technoleg a gwasanaethau penodol ar gyfer adnabod ac atal newid i'n amgylchedd sydd â photensial i fod yn niweidiol, monitro'r rhwydwaith am weithgareddau amheus ac adnabod meddalwedd sydd angen eu diweddaru;
- Buddsoddi mewn technoleg hydwyth;
- Defnyddio gwasanaethau trydydd parti i werthuso'n darpariaeth;
- Cadw polisïau diogelwch technoleg gwybodaeth yn gyfredol a cydymffurfio iddynt;
- Cynnal ymarferiadau i addysgu a chodi ymwybyddiaeth ein defnyddwyr o beryglon ac ymarfer da a pholisïau y dylid eu dilyn.

3. Risgiau a mesurau i'w lliniaru

3.1 O safbwynt technoleg gwybodaeth, colli data neu colli fynediad at ddata yw'r risg â'r effaith uchaf i'r Cyngor gan y gallai hynny arwain at allu'r Cyngor i ddarparu gwasanaethau i'r cyhoedd. Mae'n hanfodol fod y Cyngor yn cymryd camau i atal, a gallu ymateb yn effeithiol, i'r risgiau yma. Gweler isod esiamplau o'r risgiau sy'n wynebu'r Cyngor.

3.2 **Adnoddau'n wynebu'r byd cyhoeddus**: Mae darparu gwasanaethau i unigolion, grwpiau a sefydliadau, â hynny mewn amrywiaeth o leoliadau, yn golygu fod rhyngwynebau rhai systemau'n wynebu'r cyhoedd, gan gyflwyno agoriad i unigolion neu sefydliadau â bwriadau gelyniaethus.

Trefniadau Gwynedd: Mae prosesau a gweithdrefnau rhaglennu y Cyngor yn dilyn y safonau penodol i'n diogelu rhag ymyrraeth â bwriad gelyniaethus, a mae system monitro ac asesu am wendidau mewn lle sydd yn ffurf effeithiol i sicrhau fod y prosesau hynny yn cael eu dilyn heb eithriad.

3.3 **Atal Gwasanaethau**: Byddai ymgyrch *atal sefydliad rhag rhedeg gwasanaeth* ("*Denial of Service*") yn gallu cael ei wireddu drwy drefnu bod gorlwyth o draffig yn cael ei yrru i'r gwasanaethau digidol hynny sy'n wynebu'r cyhoedd a bod y gormodedd hynny'n fwy na all ein systemau ymdopi a hwy. Yn aml, byddai ymosodwyr yn defnyddio cyfres o gyfrifiaduron o dan eu rheolaeth ar gyfer cynnal ymosodiad o'r fath a byddai'n hanfodol bod gwarchodfeydd ar berimedr isadeiledd yn gallu adnabod ymosodiadau o'r fath gan atal y traffig cyn iddo ddod yn niweidiol.

Trefniadau Gwynedd: Mae systemau mewn lle sy'n edrych yn gyson am y math yma o weithgaredd ar yr haenau amrywiol o berimedrau rhwydwaith y Cyngor. Mae'r rhain wedi eu dylunio i adnabod gweithgareddau fyddai'n gallu amharu ar wasanaethau ac eu atal rhag cyflawni hynny.

3.4 **Deunydd Maleisus**: Gall deunydd maleisus ddod mewn llawer ffurf, a'i effeithiau yn amrywio o anghyfleuster ysgafn i anallu sefydliadau i weithredu. Esiampl adnabyddus o ffurf o feddalwedd o'r fath yw meddalwedd pridwerth ("ransomware"). Byddai meddalwedd yn cael ei osod ar gyfrifiadur gan seibr derfysgwyr gyda'r bwriad o greu malais gan amgryptio data'r cyfrifiadur fel nad oes modd ei ddarllen na'i ddefnyddio, byddai'r meddalwedd maleisus yn lledaenu i gyfrifiaduron a storfeydd cysylltiedig gan amgryptio pob gronyn o ddata ar ei siwrne. Cymhelliad ymosodiad o'r fath yw i droseddwr fynnu taliad pridwerth cyn dadgryptio'r data. Gyda'r pridwerth fel arfer yn mynnu cael eu talu mewn arian crypto, megis bitcoin, fel bod modd i'r troseddwyr gadw'n anhysbys.

Mae nifer o gamau i'w cymryd i liniaru'r risgiau sy'n perthyn i hyn, yn amrywio o atal y meddalwedd rhag cyrraedd peiriannau yn y lle cyntaf, amharu ar ei allu i weithredu, a trefnu bod mesurau adfer effeithiol yn bodoli petai ffeiliau yn cael eu difrodi.

Trefniadau Gwynedd: Mae gan y Cyngor brosesau a systemau i adnabod ac analluogi deunydd maleisus, hynny yn cynnwys rhaglenni hidlo traffig ac e-bost, rhaglenni gwrth-firws ac atal gweithgareddau amheus, a gweithdrefnau o ymarfer da megis rheoli'r nifer o gyfrifon sydd a uwch-hawliau. Mae pwyslais gref o adfer pe byddai ymosodiad llwyddiannus a mae trefniadau mewn lle i sicrhau bod copïau wrth-gefn, sy'n cynnwys sawl fersiwn o ffeiliau petai angen adfer colledion ar i ddyddiad penodol. Byddwn hefyd yn cynnal ymarferion parhaus i hysbysu ac atgoffa cydweithwyr am y risgiau mewn perthynas â deunydd fel hyn.

3.5 **Systemau Bregus**: Mae adnabod ac amlygu gwendidau mewn eitemau o feddalwedd yn ddiwydiant mawr, ac mae'n hanfodol bod cyflenwyr meddalwedd yn creu a darparu cyweiriadau amserol cyn i unigolion neu sefydliadau â bwriadau gelyniaethol gymryd mantais o'r gwendidau hynny i'w mantais eu hunain. Mae'n hanfodol bod pob eitem o feddalwedd â chytundeb cefnogaeth gyda'r darparwyr i baratoi a derbyn cyweiriadau mewn ymateb i ddigwyddiadau diogelwch, a wedi iddynt gael eu rhyddhau mae'n angenrheidiol i'r Cyngor osod y cyweiriadau mewn modd amserol.

Trefniadau Gwynedd: Mae gan y Cyngor systemau mewn lle i adnabod meddalwedd sydd angen eu diweddaru a phrosesau yn eu lle i lawrlwytho a mewnosod y diweddariadau hynny a phrosesau ychwanegol wedi eu sefydlu i gynnal asesiadau am statws a fersiynau ein meddalwedd i sicrhau nad oes methiannau.

3.6 **Gwe-rwydo**: Mae 'gwe-rwydo' yn derm â ddefnyddir i ddisgrifio'r gweithgaredd gelyniaethus o anfon neges (e.e. e-bost) at rywun mewn gobaith y byddai'r derbynnydd yn gweithredu mewn rhyw ffordd fyddai o fantais i'r anfonwr. Mae angen bod yn wyliadwrus o'r risg yma pan yn derbyn negeseuon gan ystyried pob tro os oes nodweddion amheus amdano. Yn anffodus, mae cynnydd gwirioneddol yn y math yma o ymosodiadau, a'r nifer sy'n disgyn am y sgamiau.

Trefniadau Gwynedd: Mae gan y Cyngor system hidlo e-bost mewn lle sydd yn asesu addasrwydd cynnwys neges ynghyd a'i ffynhonnell o safbwynt risg. Yn ogystal â hyn, mae trefniadau cyfnodol mewn lle i hysbysu ac atgoffa cydweithwyr am risgiau, fel y gallent ymateb mewn ffordd addas petai neges o'r fath yn eu cyrraedd. Mae ymarferiad penodol wedi ei drefnu eleni ar gyfer trydydd chwarter y flwyddyn 2021/22 i weld pa mor effro yw gweithlu'r Cyngor i negeseuon gwe-rwydo.

3.7 **Methiant Parhad Gwasanaeth**: Mae'r galw am, a'r dibyniaeth ar dechnoleg wedi codi'n sylweddol mewn blynyddoedd diweddar. Ymhellach, mae'r cyfnod argyfwng Covid-19 wedi cadarnhau hynny, ac mae disgwyliadau ein defnyddwyr o'r gwasanaeth a roddir iddynt wedi codi. Disgwylir bod y gwasanaeth ar gael drwy'r amser, felly mae gwaith cynnal a chadw wedi'i gynllunio oddi allan i oriau craidd, i leihau aflonyddwch ar wasanaethau. I gynnal amgylchedd sy'n cwrdd â disgwyliadau swyddogion y Cyngor a'n defnyddwyr gwasanaeth, mae'n hanfodol bod y ddarpariaeth yn hydwyth. Golygai hynny gynllunio dulliau o gyflawni'r angen mewn amgylchiadau ble bydd systemau wedi ei cyfaddawdu neu ddim ar gael o gwbl. O safbwynt technoleg gwybodaeth, golygai hyn sicrhau fod systemau, adnoddau cefnogol a darpariaeth wrth-gefn mewn lle.

Trefniadau Gwynedd: Mae prosiect yn parhau ar gyfer ymestyn argaeledd systemau allweddol y Cyngor. Cyflwynir gwasanaethau gweinyddwyr rhithwir o ddwy ganolfan data gyda gwasanaethau'n parhau pe byddai methiant i un o'r canolfannau yma.

3.8 **Methiant Ymateb i Ddigwyddiadau**: Y dull mwyaf effeithiol o brofi effeithiolrwydd camau lliniaru yw drwy gynnal ymarferion ail-greu amgylchiadau fyddai â photensial i fod yn niweidiol, gan asesu llwyddiant yr ymarferiad i atal neu leihau'r amhariad. Gall amgylchiadau digwyddiad amrywio yn fawr, felly mae'n hanfodol i gynllunio i fanylder ynghyd ag adolygu a datblygu ein mesurau ymateb.

Trefniadau Gwynedd: Mae hyn yn rhan allweddol mewn ymgorffori rhai o'r camau sydd wedi eu disgrifio yn y ddogfen yma ac mae'n broses cyson. Mae'r Cyngor yn gweithio gydag asiantaethau eraill i sefydlu cynlluniau argyfwng ac ymarferion ymateb i ddigwyddiadau amrywiol fel rhan o'i ddyletswydd cynllunio argyfwng.

4. Achrediadau

4.1 **Rhwydwaith Gwasanaethau Cyhoeddus *(Public Services Network*, "PSN")**: Pwrpas y PSN yw gweithredu fel rhwydwaith annibynnol i'n rhwydwaith gorfforaethol ac yn cael ei rannu gan amryw o wasanaethau cyhoeddus cenedlaethol ar draws y Deyrnas Unedig.

4.2 Mae'r Cyngor angen cysylltu â'r rhwydwaith yma er mwyn darparu rhai gwasanaethau hanfodol, yn benodol yn y meysydd budd-daliadau a chefnogaeth oedolion. Un o prif egwyddorion y PSN yw'r angen i ymddiried yn oll o'r sefydliadau sydd wedi cysylltu i rwydwaith y PSN, ac i'r perwyl hwnnw mae angen cyrraedd safonau penodol o safbwynt diogelwch. Fe waherddir cyswllt pe na byddai achrediad cyfredol.

4.3 Fe gyflwynir cais i gysylltu i rhwydwaith y PSN i Swyddfa'r Cabinet (Llywodraeth y Deyrnas Unedig), yn eu rôl fel ceidwad y rhwydwaith, gan gyflwyno tystiolaeth penodol sy'n cynnwys asesiad diogelwch gan gwmni trydydd parti ardystiedig a chynllun i adfer unrhyw eitemau risg uchel fu ei ddarganfod.

4.4 Bu i'r Cyngor sicrhau ei achrediad presennol ym Mai, 2021. Mae achrediad o'r fath yn rhoi sicrwydd annibynnol o lefel a mesurau diogelwch sydd wedi eu sefydlu gan y Cyngor.

5. PSBA (Public Sector Broadband Aggregation)

5.1 Menter Cymru gyfan yw'r PSBA i gyflwyno rhwydwaith ardal eang sydd wedi ei ddylunio ar gyfer a gan wasanaethau y sector gyhoeddus. Roedd Cyngor Gwynedd yn un o ddefnyddwyr cyntaf y PSBA, ac rydym yn parhau i gyfrannu ar gyfeiriad strategol a thechnegol y rhwydwaith.

5.2 Mae'r PSBA yn galluogi byrddau iechyd lleol, awdurdodau lleol, sefydliadau addysg uwch a phellach, gwasanaethau brys golau glas, a chyrff cyhoeddus eraill i ddarparu gwasanaethau effeithlon ar gyfer y boblogaeth, drwy ddefnyddio gwasanaethau rhwydwaith arloesol, cost effeithiol, dibynadwy gan dderbyn cyfeiriad gan fyrddau penodol sy'n cynnwys cynrychiolaeth ar draws y sector, gan gynnwys Cyngor Gwynedd.

5.3 Mae diogelwch yn gynhennid i'r gwasanaeth yma, gan gynnig amddiffynfeydd ychwanegol i'r hyn sydd ar ymyl ac oddi fewn i rwydwaith y Cyngor ac yn gweithredu fel sylfaen sy'n cefnogi gweddill ein isadeiledd.

6. Prentis

6.1 Mae'r Gwasanaeth Technoleg Gwybodaeth wedi penodi Prentis Diogelwch Seibr, drwy gynllun prentis wedi'i drefnu gan y Cyngor. Byddwn yn croesawu'r prentis i'r tîm estynedig yn Awst, 2021 gan ei rhyddhau i fynychu'r Brifysgol ar gwrs gradd B.Sc. mewn Diogelwch Seibr.

7. Ystadegau digwyddiadau

7.1 Nid yw'r Cyngor wedi dioddef colledion yn deillio o ddigwyddiad seibr diogelwch o fewn y 5 mlynedd diwethaf. Mae systemau diogelu a monitro mewn lle ar ymylon rhwydwaith y Cyngor, ac o fewn y rhwydwaith, sy'n tynnu sylw at eitemau neu weithgareddau gelyniaethus. Mae digwyddiadau o'r fath yn gyson, gyda negeseuon e-bost amheus, sganiau dirgel am wybodaeth technegol ac ymgeisiadau i ymosod ar ein adnoddau yn weithgaredd arferol dyddiol, yn hytrach na rhywbeth anghyffredin.

8. Cloi

8.1 Cynyddu fydd y gweithgareddau gelyniaethus hyn ac er ein ymdrechion i amddiffyn ein isadeiledd a'n systemau o ymosodiad gan derfysgwyr seibr, ni ellir rhoi gwarant 100% bod modd atal pob ymdrech. Rydym eisoes wedi nodi bod ein ymdrechion ar gyfer gwytnwch ein gwasanaethau yn gyfuniad o amddiffynfeydd seibr a'n gallu i adfer o sefyllfa pe byddai ymosodiad yn torri trwy'r amddiffynfeydd. Mae hyn yn cael ei adlewyrchu ar y gofrestr risg corfforaethol, gan nodi risg o debygolrwydd lled isel (2) ac effaith uchel iawn (5).