Strategaeth Seibrgadernid 2022 - 2027

CONWY
CYNGOR BWRDEISTREF SIROL
COUNTY BOROUGH COUNCIL

Conwy - Sir flaengar sy'n creu cyfleoedd

Conwy - a progressive County creating opportunity

Tabl Cynnwys

1. Rhagair

Mae gwybodaeth a data'n hanfodol i bob agwedd o ddarparu gwasanaethau Cyngor Bwrdeistref Sirol Conwy. Wrth i ni barhau gyda'n huchelgeisiau Trawsnewid Digidol i foderneiddio'r ffordd rydym yn gweithio a chynnig rhagor o ddewis i bobl ar sut i gael mynediad at wybodaeth a gwasanaethau, mae arnom ni angen mesurau diogelwch cadarn i ddiogelu yn erbyn bygythiadau seibr ac amhariadau i'n seilwaith Technoleg Gwybodaeth (TG).

Yn fyd-eang, mae ymosodiadau seibr yn digwydd yn fwy aml ac maent yn fwy soffistigedig. Pan fyddant yn llwyddo, gall y difrod newid bywydau; gyda goblygiadau personol, economaidd a chymdeithasol difrifol.

Mae'r Strategaeth Seibrgadernid hon yn amlinellu ein dull ar gyfer diogelu ein systemau gwybodaeth a'r data maent yn ei gadw i sicrhau bod y gwasanaethau rydym yn eu darparu mor ddiogel â phosibl. Mae'n hanfodol bod ein dinasyddion, busnesau, ymwelwyr a budd-ddeiliaid yn gallu trafod a rhyngweithio gyda ni yn ddiogel. Mae hyn yn cynnwys cyflawni cydbwysedd o groesawu cyfleoedd digidol, gan gynnwys sicrhau bod gwybodaeth ar gael ac yn fwy hygyrch i ystod eang o bobl, a sicrhau bod y lefelau diogelu cywir ar waith.

Mae'r strategaeth hon yn amlinellu ein hymrwymiad a'r camau allweddol y byddwn yn eu cymryd dros y pum mlynedd nesaf i ddatblygu amgylchedd digidol dibynadwy ar gyfer Conwy. Byddwn yn cryfhau a diogelu'r Cyngor rhag bygythiadau seibr drwy fuddsoddi yn ein systemau a'n seilwaith, atal gwrthwynebwyr, a datblygu ystod eang o ymatebion; o hylendid seibr sylfaenol i'r amddiffyniadau mwyaf soffistigedig. Byddwn hefyd yn sicrhau ein bod wedi paratoi i ddelio â phroblemau allai achosi amhariadau sylweddol i systemau a seilwaith TG.

Bydd ymosodiadau seibr yn parhau i esblygu, ac o'r herwydd, byddwn yn parhau i fod ar flaen y gad mewn perthynas â bygythiadau. O ystyried y ddibyniaeth gynyddol ar TG ynghyd ag amlder a chymhlethdod ymosodiadau seibr, byddwn yn sicrhau bod prosesau ar waith i helpu i sicrhau cyn lleied â phosibl o effaith ar wasanaethau mewn achosion o ymosodiadau llwyddiannus neu amhariadau sylweddol i'n seilwaith a'n systemau TG.

Mae'r Strategaeth Seibrgadernid hon yn ategu Strategaeth Ddigidol Conwy; sydd yn amlinellu sut bydd y Cyngor yn gwneud y mwyaf o dechnoleg i gyflawni ei weledigaeth o ddatblygu Conwy fel Sir flaengar sy'n creu cyfleoedd. At hynny, mae'n cyfrannu at flaenoriaeth gorfforaethol Conwy o sicrhau fod pobl yng Nghonwy yn ddiogel ac yn teimlo'n ddiogel drwy sicrhau ein bod yn cymryd camau i ddiogelu data personol a hyrwyddo seibr ddiogelwch er mwyn sicrhau bod ein dinasyddion yn aros yn ddiogel ar-lein.

Bydd y mesurau a amlinellir yn y strategaeth hon yn diogelu ymddiriedaeth a hyder yn y modd rydym ni'n gweithredu ac yn darparu ein gwasanaethau, gan gefnogi Conwy i fod ar flaen y gad o ran y chwyldro digidol.

Y Cynghorydd Charlie McCoubrey,
Arweinydd Cyngor Bwrdeistref Sirol Conwy

CONWY
CYNGOR BWRDEISTREF SIROL
COUNTY BOROUGH COUNCIL

CONWY
CYNGOR BWRDEISTREF SIROL
COUNTY BOROUGH COUNCIL

2. Cyflwyniad

Mae'r ddogfen hon yn nodi defnydd Cyngor Bwrdeistref Sirol Conwy o fesurau seibrgadernid sy'n diogelu ein systemau gwybodaeth, y data y cedwir arnynt a'r gwasanaethau rydym yn eu darparu rhag amhariad sylweddol, mynediad diawdurdod, niwed, neu gamddefnydd.

Dyma ein hymrwymiad i ddinasyddion, ymwelwyr, busnesau, partneriaid, swyddogion ac aelodau y Sir yn ogystal â'n hymrwymiad i gynnal systemau a data diogel er budd lleol a chenedlaethol.

3. Beth yw Seibrgadernid a pham mae'n bwysig?

Seibrgadernid yw'r gallu i baratoi ar gyfer, ymateb i, ac adfer yn dilyn ymosodiadau seibr neu amhariadau ehangach i systemau neu seilwaith TG y Cyngor a allai gael effaith ar ein gwasanaethau.

Mae wedi dod yn fwy perthnasol dros y blynyddoedd diwethaf gan nad yw mesurau diogelwch seibr traddodiadol bellach yn ddigon i ddiogelu sefydliadau rhag y gyfres o ymosodiadau cyson, mae hefyd yn hollbwysig bod y Cyngor yn gallu arddangos gwytnwch mewn achosion o amhariadau sylweddol i systemau TG.

Mae seibr ddiogelwch yn ymwneud yn benodol â sicrhau cyfrinachedd, uniondeb ac argaeledd gwybodaeth.

- **Ymosodiadau ar Gyfrinachedd** – dwyn, neu yn hytrach copïo gwybodaeth bersonol.
- **Ymosodiadau ar Gywirdeb** – ceisio llyfru, difrodi neu ddinistrio gwybodaeth neu systemau a'r bobl sydd yn dibynnu arnynt.
- **Ymosodiadau ar Argaeledd** – gwrthod gwasanaethau, caiff ei weld ar ffurf meddalwedd wystlo neu drwy gyfnod hir o ymosodiadau ar wasanaethau i amharu ar fynediad ehangach i systemau.

Mae seibrddiogelwch yn cyfeirio at gorff o dechnolegau, prosesau, ac arferion sydd wedi'u dylunio i amddiffyn rhwydweithiau, dyfeisiau, rhaglenni a data rhag ymosodiad, difrod neu fynediad diawdurdod. Gellir cyfeirio at seibrddiogelwch fel diogelwch TG hefyd.

Mae seibrddiogelwch yn bwysig achos er mwyn darparu gwasanaethau'n effeithiol mae Cyngor Conwy yn casglu, prosesu ac yn storio llawer o ddata ar systemau, cyfrifiaduron a dyfeisiau eraill yn ein canolfannau data neu mewn canolfannau data (cwmwl) a gaiff eu cynnal yn allanol. Mae cyfran fawr o'r data yma'n wybodaeth sensitif, yn cynnwys data ariannol, gwybodaeth bersonol, neu fathau eraill o ddata allai arwain at oblygiadau negyddol petai rhywun yn cael mynediad diawdurdod neu petai'n cael ei ddatgelu.

Mae Cyngor Bwrdeistref Sirol Conwy yn anfon data sensitif ar draws rhwydweithiau ac i ddyfeisiau eraill wrth ddarparu gwasanaethau. Seibrddiogelwch yw'r ddisgyblaeth sy'n benodol i ddiogelu'r wybodaeth yma a'r systemau a ddefnyddir i brosesu neu ei storio.

Mae mabwysiadu mesurau Seibrgadernid da'n hanfodol ar gyfer sicrhau bod gwasanaethau'n cael eu cynnal a'u paratoi ar gyfer ymosodiad neu amhariad posibl i systemau. Mae hefyd yn hollbwysig er mwyn sicrhau bod y cyhoedd yn ymddiried yn y Cyngor gyda'u gwybodaeth. Gall ymosodiad seibr arwain at oblygiadau difrifol iawn, drwy amharu ar wasanaethau, sy'n darparu ar gyfer ein dinasyddion mwyaf diamddiffyn, yn ogystal â gwneud niwed i enw da'r Cyngor.

4. Cyd-destun Strategol

Y weledigaeth drosfwaol yng Nghynllun Corfforaethol y Cyngor yw “Conwy - Sir flaengar sy’n creu cyfleoedd”. Rydym yn gweithio mewn awyrgylch sy’n newid ac sy’n gofyn llawer. Ein gweledigaeth yw bod yn flaengar wrth reoli newid a’i ddefnyddio i greu cyfleoedd; i warchod yr hyn sydd gennym ac i adeiladu ar hyn er mwyn delio â newid. Mae’r weledigaeth hon yn ymdrech a rennir. Rydym eisiau cryfhau ein perthynas gyda dinasyddion er mwyn ein galluogi i weithio gyda’n gilydd i wella’r sir. Yn y cyfan a wnawn, o addysgu plant, gofalu am bobl ddiamddiffyn, ailgylchu gwastraff, rheoleiddio busnesau, i ddarparu cyfleusterau hamdden a pherfformiadau theatr i enwi ond ychydig, maent eisiau bod yn flaengar a chreadigol er mwyn i ni fanteisio ar y cyfleoedd sydd ar gael i’r cymunedau yn Sir Conwy.

Mae’r cynllun nodi sut byddwn yn gwneud y defnydd gorau o dechnoleg ddigidol a sianeli digidol i ddarparu mynediad mwy effeithiol ac effeithlon at wasanaethau. Mae hefyd yn egluro y byddwn yn manteisio hyd yr eithaf ar ddatblygiadau mewn technoleg i drawsnewid y ffordd y mae ein staff yn gwneud eu gwaith o ddydd i ddydd gan edrych ar y teclynnau/offer y maent yn eu defnyddio yn ogystal â’u cyfleusterau a’r lleoliadau ble maent yn gweithio ynddynt/ohonynt.

Mae’r Strategaeth Seibrgadernid hon yn cefnogi darparu’r Cynllun Corfforaethol (2022-2027) a’r Strategaeth Ddigidol (2022-2027) drwy ddarparu fframwaith i’r Cyngor i harneisio manteision y chwyldro digidol er budd pob budd-ddeiliaid yn ddiogel. Mae’n hanfodol i rediad ac esblygiad effeithlon y Cyngor.

Mae’r Strategaeth Seibrgadernid yn mynd law yn llaw gyda’r Strategaeth Ddigidol ac yn cael ei gefnogi gan gyfres o bolisïau gweithredol sydd yn llywodraethu sut y dylai swyddogion a gwasanaethau ddefnyddio technoleg a systemau a gynhelir yn lleol neu’n allanol mewn modd saff a diogel.

5. Diben a Chwmpas

Mae Strategaeth Ddigidol y Cyngor wedi amlinellu pedwar prif faes blaenoriaeth gan dargedu datblygu Sir Ddigidol - Gweithlu Digidol, Gwasanaethau Digidol, Cysylltedd Digidol ac Economi Ddigidol. Mae graddfa'r newid yn cynrychioli symudiad sylweddol yn y daith i drawsnewid y Cyngor yn ddigidol.

Mae'r Strategaeth Seibrgadernid wedi cael ei lunio mewn ymateb i nifer o ymosodiadau seibr llwyddiannus ac o broffil uchel ar sefydliadau cyhoeddus a phreifat. Pwrpas y strategaeth yw rhoi sicrwydd i bobl sy'n defnyddio gwasanaethau'r Cyngor a budd-ddeiliaid eraill o'n hymrwymiad i ddarparu mesurau diogelwch gwybodaeth cadarn i ddiogelu data rhag cael ei gamddefnyddio a bygythiadau seibr. Y nod yw diogelu eu preifatrwydd drwy drefniadau llywodraethu gwybodaeth a rhannu data sydd yn fwyfwy diogel a modern - yn fewnol a gyda phartneriaid.

Drwy ddarparu'r strategaeth hon, byddwn yn cydymffurfio gydag ac yn sefydlu egwyddorion 'Cyber Essentials'; cynllun Canolfan Seibrddiogelwch Cenedlaethol a gefnogir gan y llywodraeth a diwydiant i helpu sefydliadau i ddiogelu eu hunain rhag bygythiadau cyffredin ar-lein. Byddwn hefyd yn dilyn y fframwaith "10 Cam i Seibrddiogelwch" a gyhoeddwyd gan y Ganolfan Seibrddiogelwch Genedlaethol (sydd wedi'i gynnwys yn Atodiad 2).

Bwriedir i'r strategaeth hon gynnwys holl systemau gwybodaeth Cyngor Bwrdeistref Sirol Conwy, y data y cedwir arnynt, a'r gwasanaethau maent yn helpu i'w darparu. Mae hefyd yn nodi'r ffyrdd y bydd y Cyngor yn hyrwyddo seibrddiogelwch i ddinasyddion i'w helpu i'w cadw'n ddiogel ar-lein.

6. Yr Her

Mae Cyngor Bwrdeistref Sirol Conwy yn defnyddio amrywiaeth gynyddol o ddatrysiadau a seilwaith technoleg yn cynnwys ein gwefannau, systemau rheoli ac apiau sydd ar gael o ystod eang o ddyfeisiau yn cynnwys gliniaduron, cyfrifiaduron, tabledi neu ffonau clyfar.

Mae agweddau cynyddol o'n gwasanaethau a systemau yn cael eu defnyddio ar-lein: ysgrifennu at breswylwyr a busnesau lleol, gwneud gwaith achos, darparu cefnogaeth trwy ganolfannau cyswllt, cynnig gwasanaethau a thaliadau dros y we, adolygu adroddiadau neu bapurau ar gyfer cyfarfodydd y cyngor a chyfarfod ar lwyfannau digidol.

Mae disgwyl i'r arferion yma barhau a chyflymu; gan olygu bod mesurau seibrgadernid effeithiol hyd yn oed yn fwy hanfodol er mwyn amddiffyn yn erbyn mathau newydd o fygythiadau, risgiau a diamddiffynedd a sicrhau bod gan y Cyngor yr adnoddau i adfer os bydd amhariad sylweddol.

Mae canllawiau Llywodraeth y DU a Llywodraeth Cymru'n cynghori bob corff cyhoeddus i baratoi ar gyfer goblygiadau ymosodiadau seibr llwyddiannus ac amhariadau sylweddol i fynediad at systemau TG.

Mae'n gyfrifoldeb ar bob adran o'r Cyngor i fod yn wyliadwrus ac yn ymwybodol o'r risgiau o ymosodiadau ac amhariadau seibr posibl. O ystyried cymhlethdod a graddfa gynyddol ymdrechion diawdurdod i niweidio neu ymdreiddio i systemau - mae'n rhaid i ni weithio ar sail "nid os, ond pryd" fydd ymosodiad yn achosi amhariad sylweddol i wasanaethau, ac mae'n hanfodol sicrhau ein bod yn barod ar gyfer digwyddiad o'r fath.

7. Bygythiadau

Os na chaiff bygythiad ei wirio, fe allai amharu ar weithrediad y Cyngor o ddydd i ddydd, darparu gwasanaethau cyhoeddus lleol ac yn y pendraw, posibilrwydd y gallai beryglu diogelwch cenedlaethol.

Mae yna amrywiaeth o fygythiadau y mae'n rhaid i'r Cyngor eu hystyried a chymryd camau i amddiffyn yn eu herbyn yn rhan o unrhyw Strategaeth Seibrgadernid ac i sicrhau bod mesurau seibr ddiogelwch effeithiol ar waith pa unai ydi systemau'n cael eu cynnal yng nghanolfannau data Conwy neu'n allanol gan drydydd parti.

Math o Fygythiad	Manylion
A) **Seibr droseddwyr a throseddau seibr**	Ar y cyfan, mae seibr droseddwyr yn gweithio er mwyn elwa'n ariannol. Yn fwyaf cyffredin, at ddibenion twyll: naill ai'n gwerthu gwybodaeth y maent wedi'i gael trwy ddulliau anghyfreithlon i drydydd parti, neu ei ddefnyddio'n uniongyrchol at ddibenion troseddol. Mae'r prif adnoddau a dulliau a ddefnyddir gan seibrdroseddwyr yn cynnwys: • Maleiswedd – meddalwedd maleisus sy'n cynnwys firysau, Trojan, Worm neu unrhyw god neu gynnwys allai gael effaith andwyol ar sefydliadau neu unigolion • Meddalwedd wystlo – math o faleiswedd sydd yn cloi dioddefwyr allan o'u data neu systemau a dim ond yn rhoi mynediad yn ôl iddynt pan fyddant wedi talu • Gwe-rwydo – e-byst sy'n smalio dod gan asiantaeth gyhoeddus i echdynnu gwybodaeth sensitif gan aelodau o'r cyhoedd.
B) **Hacio**	Gall hacwyr geisio cael mynediad at systemau bregus fel her neu i dynnu sylw at ddiffygion diogelwch. Yn gyffredinol bydd hacwyr yn ceisio cymryd rheolaeth o wefannau cyhoeddus neu gyfrifon cyfryngau cymdeithasol er mwyn codi proffil am achos penodol. Pan fyddant yn cael eu targedu yn erbyn gwefannau a rhwydweithiau llywodraeth leol, gall yr ymosodiadau yma achosi niwed i enw da yn lleol. Os caiff gwasanaethau eu hamharu gan ymosodiadau seibr, fe allai hyn arwain at golli ymddiriedaeth y cyhoedd i ddefnyddio gwasanaethau o'r fath. Mae grwpiau hacio wedi defnyddio ymosodiadau atal gwasanaeth sy'n wasgaredig yn llwyddiannus (DDoS - pan fydd system, gwasanaeth neu rwydwaith o dan gymaint o fyrdwn i'r fath raddau gan ymosodiadau electronig, nid oes modd ei ddefnyddio) er mwyn amharu ar wefannau nifer o gynghorau'n barod.
C) **Mewnwyr (Swyddogion, Partneriaid ac Aelodau o fewn y Cyngor)**	Gall swyddogion neu aelodau ddatgelu gwybodaeth sensitif neu ddata yn gyhoeddus yn fwriadol neu'n anfwriadol. Fe allai hyn fod at ddiben tanseilio neu i werthu i barti arall serch hynny mae'r achos mwyaf cyffredin yn gysylltiedig â gwallau dynol neu ddiffyg ymwybyddiaeth am y risgiau penodol sy'n rhan ohono.
D) **Bygythiadau Diwrnod Sero**	Camfantais diwrnod sero yw ymosodiad seibr sydd yn digwydd ar yr un diwrnod y mae gwendid yn cael ei ganfod mewn meddalwedd. Bryd hynny, caiff ei ecsbloetio cyn bod modd i'r darparwr meddalwedd ei drwsio a chyn i systemau amddiffyn megis cynnyrch gwrth-feirws gael eu diweddaru gyda'r wybodaeth ddiweddaraf er mwyn ei amddiffyn rhag y math o ymosodiad. Mae'n ymosodiad sydd yn camfanteisio ar fregusrwydd diogelwch na wyddem amdano gynt. Mae hyn yn achosi risg i unrhyw gyfrifiadur neu system sydd heb gael ddiweddariad priodol, neu wedi diweddaru ei feddalwedd gwrth-feirws.

Math o Fygythiad	Manylion
E) **Colli canolfan(nau) data neu seilwaith**	Mae'r ddibyniaeth gynyddol ar wasanaethau digidol yn arwain at fregusrwydd cynyddol os bydd tân, llifogydd, toriad pŵer neu drychineb naturiol arall neu rywbeth arall sydd yn effeithio ar systemau TG y Cyngor. Mae gweithredu canolfannau data cadarn, diogel yn hanfodol ar gyfer parhad gwasanaeth.
F) **Ysbio**	Mae llawer o'r asiantaethau cudd-wybodaeth tramor mwyaf soffistigedig a gelyniaethus yn targedu rhwydweithiau llywodraeth y DU a'r sector cyhoeddus i ddwyn gwybodaeth sensitif. Fe allai amharu ar linellau cyfathrebu a chysylltedd rhyngrwyd i gyfyngu ar allu'r DU i gynnal busnes gael oblygiadau difrifol.
G) **Sefydliadau Terfysgol**	Mae rhai grwpiau terfysgol yn arddangos bwriad i gynnal ymosodiadau seibr. Fe allai grwpiau terfysgol gael medrusrwydd gwell mewn nifer o ffyrdd, drwy rannu arbenigedd mewn fforymau ar-lein sydd yn darparu cyfle sylweddol i derfysgwyr gynyddu eu medrusrwydd.

8. Diamddiffynedd

Diamddiffynedd yw gwendidau neu gyflyrau eraill mewn sefydliad y gall gweithredwr bygythiadau; megis haciwr, cenedl-wladwriaeth, gweithiwr anfodlon, neu ymosodwr arall, eu hecsbloetio er mwyn cael effaith andwyol ar ddiogelwch data.

Yn nodweddiadol mae diamddiffynedd seibr yn cynnwys is-set o'r gwendidau hynny ac yn canolbwyntio ar faterion yn y meddalwedd TG, caledwedd a systemau y mae sefydliad yn ei ddefnyddio.

- **Cynnal a Chadw System** - Dylai meddalwedd sy'n cael ei gynnal mewn canolfannau data ac ar ddyfeisiau gael ei ddiweddaru a'i wirio'n rheolaidd ac yn effeithiol. Mae hi'n hanfodol bod y systemau'n cael eu diweddaru'n llwyr gyda'r amddiffyniad diogelwch diweddaraf a bod datrysiadau priodol yn cael eu gosod. Mae gosodiad gwael, camreolaeth, neu faterion eraill yn y modd y mae sefydliad yn gosod ac yn cynnal ei galedwedd TG a chyfansoddion meddalwedd yn fygythiad.

- **Cynnal a Chadw Seilwaith** - Mae cynnal swyddogaeth graidd TGCh o fewn amgylchedd diogel, gyda diweddariadau diogelwch a chynlluniau cynnal a chadw priodol ar waith yn ystyriaethau hanfodol hefyd.

- **Mynediad i Feddalwedd** – Er mwyn sicrhau bod gan systemau dilysrwydd defnyddiwr a system digonol, gwiriad dilysrwydd data neu nodweddion gwirio cywirdeb data sydd yn atal mynediad diawdurdod i systemau.

- **Hyfforddiant a Sgiliau** – Mae'n hollbwysig bod yr holl weithwyr, aelodau a phartneriaid yn deall seibrddiogelwch a sut y dylai eu harferion gweithio gefnogi hyn. Gall hyrwyddo ymwybyddiaeth ymysg dinasyddion o ran cadw'n ddiogel ar-lein helpu i leihau risgiau o golli gwybodaeth bersonol hefyd.

9. Risgiau

Mae Rheoli Risg Seibr yn rhan sylfaenol o reoli'r risg ehangach er mwyn sicrhau bod heriau seibr ddiogelwch yn cael eu hadnabod yn llawn ar draws y Cyngor a bod gweithred briodol yn cael ei gynnal i liniaru'r risg.

Yng Nghyngor Bwrdeistref Sirol Conwy, mae risgiau seibr ddiogelwch a goblygiadau ymosodiad yn cael eu cofrestru ar y gofrestr risgiau gorfforaethol. Mae rhagor o risgiau seibrddiogelwch a chadernid cysylltiedig hefyd yn cael eu nodi yn y gofrestr risg TG a Thrawsnewid Digidol.

Mae adolygu risgiau a mesurau lliniaru yn rheolaidd er mwyn cynnal lefelau priodol o amddiffyniad yn allweddol i wneud y mwyaf o lefelau o amddiffyniad y Cyngor yn erbyn amhariad i systemau TG ac achosion posibl o golli data.

Mesur lliniaru allweddol yw helpu i ddelio â goblygiadau ymosodiadau risg a/neu gyfnod sylweddol o amhariad i systemau TG yw bod Gwasanaethau yn sicrhau eu bod yn cynnwys darpariaeth i weithredu'n effeithiol heb fynediad i systemau TG neu wasanaethau, yn cynnwys camau i boblogi systemau gyda gwybodaeth pan fydd y gwasanaethau TG wedi cael eu hadfer.

10. Ein Dull, Egwyddorion a'n Blaenoriaethau

Er mwyn lliniaru yn erbyn y nifer o fygythiadau sy'n gysylltiedig â seibrgadernid y mae'r Cyngor yn eu hwynebu, mae angen dull strategol er mwyn ategu gweithredoedd cyfunol ac unigol. Bydd hynny'n cynnwys:

Sicrhau bod y bygythiad o ymosodiad seibr a cholli data neu systemau'n cael ei nodi fel risg gorfforol gan sicrhau fod ein staff, aelodau etholedig a phartneriaid yn deall cyfrifoldebau o ran gweithredoedd lliniaru risg.

Defnyddio systemau a rheolau sydd yn helpu i adnabod bygythiadau posibl, amddiffyn yn erbyn ymosodiadau a chefnogi cadernid ein seilwaith, systemau a dyfeisiau TG.

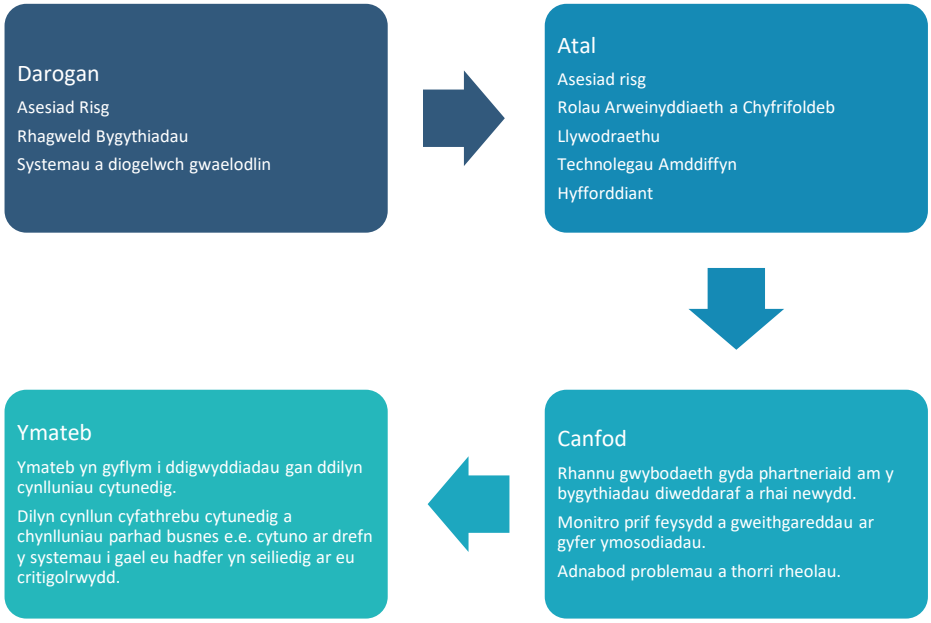
Mae hyfforddiant Ymwybyddiaeth Seibr yn helpu i liniaru bygythiadau mewnol, deall risgiau'r gadwyn gyflenwi a sicrhau fod pob swyddog yn deall y problemau a'u cyfrifoldebau.

Cynnal achrediadau priodol sydd angen adolygiadau blynyddol sy'n cael eu gweinyddu'n allanol o fesurau amddiffyn y Cyngor. Bydd y rhain yn cynnwys mabwysiadu rheolau cynllun Hanfodion Seibr a Mwy, Rhwydwaith y Gwasanaethau Cyhoeddus (PSN) a chydymffurfio â Diwydiant Cardiau Talu (PCI). Trwy weithio i gydymffurfio gyda safonau a osodir mewn fframweithiau eraill yn cynnwys elfennau o ISO 27000 fe allwn weithio i sicrhau y bydd y Cyngor yn gallu adnabod, lliniaru ac amddiffyn yn erbyn risgiau diogelwch gwybodaeth mewn modd sy'n cael ei flaenoriaethu ac sydd ag adnoddau.

Yn yr un modd, mae yna rwymedigaeth ar Wasanaethau'r Cyngor sy'n canfod systemau sy'n cael eu cynnal ar Blatfformau Cwmwl neu'n cael eu darparu drwy "Feddalwedd fel Gwasanaeth" i sicrhau bod lefelau cyfartal o sicrwydd yn cael eu cynnal.

Gosod dull darparu'r gwasanaeth o fewn cynlluniau parhad gwasanaeth os bydd ymosodiad seibr neu amhariad sylweddol a hir ar Wasanaethau TG.

Mae'r diagram isod yn dangos y prif gamau i amddiffyn y Cyngor rhag bygythiadau ac amhariadau sy'n ymwneud â seibr i wasanaethau TG:



Prif Gamau i Amddiffyn y Cyngor

11. Cynllun Gweithredu

Er mwyn addasu i'r tirlun newidiol a chyflawni ein gweledigaeth, byddwn yn alinio â dull y Strategaeth Seibrddiogelwch Genedlaethol i amddiffyn seilwaith TGCh Cyngor Bwrdeistref Sirol Conwy, systemau a data waeth pwy yw'r darparwr cynnal. Pan fydd systemau'n cael eu canfod neu eu cynnal yn allanol, dylai unrhyw gontractau sicrhau lefelau cyfartal o sicrwydd seibrgadernid sydd yn briodol i'r wybodaeth y cedwir sy'n cael ei ddarparu trwy gydol.

AMDDIFFYN

Fe fydd gan y Cyngor y dulliau o amddiffyn yn erbyn bygythiadau seibr sy'n esblygu, er mwyn ymateb yn effeithiol i ddigwyddiadau, ac i sicrhau bod rhwydweithiau, data a systemau'n cael eu hamddiffyn a'u bod yn gadarn. Mae'n cynnwys helpu ein dinasyddion, ymwelwyr, busnesau, swyddogion, aelodau etholedig a phartneriaid i gael yr wybodaeth a'r gallu i amddiffyn eu hunain.

Camau Gweithredu:

Systemau Diogelwch

- Gweithredu muriau cadarn, amddiffyn meddalwedd, canfod bygythiad a systemau sganio.
- Sicrhau amddiffyniad priodol o fewn systemau wrth gefn ac adfer.

Gwiriadau a phrofion iechyd

- Cynnal gwiriadau iechyd a phrofion hacio ar draws ein seilwaith.
- Ymarferion seibrgadernid er mwyn profi adferiad ein systemau a'n prosesau.
- Sicrhau bod cynlluniau parhad gwasanaeth yn cynnwys cyfnodau o amhariad TG.

Gweithdrefnau cydymffurfiaeth ac achrediadau

- Mae cynnal achrediadau Hanfodion Seibr a Mwy a bodloni gofynion cydymffurfiaeth ar gyfer Cod Cysylltiad y Llywodraeth (Co-Co) ar gyfer Rhwydwaith y Sector Cyhoeddus a Diwydiant Cardiau Talu sydd angen hylendid seibr da, i gysylltu gyda rhwydweithiau preifat y llywodraeth.

Gweithio gyda Phartneriaid

- Gweithio gyda phartneriaid ar draws y sector cyhoeddus drwy gymryd rhan mewn grwpiau yn cynnwys grŵp SOCITM WARP i gefnogi rhannu gwybodaeth, rhybuddio, cynghori ac adrodd.

ATAL

Mae'r Cyngor a phartneriaid yn parhau i fod yn darged ym mhob ffurf o ymosodiad yn y seibrofod. Fe fydd hyn yn golygu canfod, deall, ymchwilio a tharfu ar weithredu gelyniaethus yn erbyn seilwaith a systemau TG y Cyngor.

Camau Gweithredu:

- Defnyddio canllawiau seibr ddiogelwch y llywodraeth a seibr, e.e. Hanfodion Seibr
- Cynnal cofrestri risg er mwyn sicrhau bod seilwaith TG y Cyngor yn parhau'n gadarn ac wedi'i amddiffyn.
- Sicrhau bod amserlen o archwiliadau mewnol yn eu lle i fonitro cydymffurfiaeth gyda'r strategaeth.

- Diogelwch Rhwydwaith yn cynnwys amddiffyniad mur cadarn.
- Amddiffyniad Gwrth-firws
- Amddiffyn systemau e-bost
- Ni fydd defnyddwyr gyda braint system eang neu helaeth yn defnyddio eu cyfrifon braint ar gyfer swyddogaethau risg uchel, yn enwedig darllen e-bost a phori'r we.
- Fe ddefnyddir dilysiad sawl ffactor pan fo hynny'n dechnegol bosibl, drwy ddyfais amgryptiad ar gyfer defnyddwyr a/neu docynnau pan mae consolau gweinyddol yn darparu mynediad er mwyn gweinyddu seilwaith, platfformau neu wasanaethau.
- Dylid defnyddio cyfrineiriau cymhleth i gael mynediad i bob cyfrif gyda rheolau'n cael eu gosod i analluogi cyfrifon sydd heb eu defnyddio o fewn cyfyngiadau amser cytunedig. Bydd cyfrifon gyda lefelau uchel o fynediad i systemau'r Cyngor yn cael eu rheoli'n llym gyda chymhlethdod cyfrinair lefel uchel a llai o derfyn amser ar gyfrifon nad ydynt yn fyw.
- Bydd cyfansoddion seilwaith yn cael eu newid o werthoedd diofyn ac ni fyddant yn hawdd i'w dyfalu.
- Atal Maleiswedd
- Rheolau Cyfryngau Cludadwy
- Cynnal Polisïau TG a Diogelwch Gwybodaeth effeithiol
- Cyhoeddi arferion da ar y fewnrwyd.

- Gall addysgu defnyddwyr helpu i ganfod, atal ac amddiffyn yn erbyn bygythiadau Seibr.
- E-bostio a chyhoeddi gwybodaeth ar brif fygythiadau newydd neu rhai presennol.
- Hyrwyddo ymwybyddiaeth am gamau diogelwch seibr gyda'n dinasyddion drwy hyfforddiant a negeseuon ar gyfryngau cymdeithasol ac o lyfrgelloedd.

DATBLYGU

Bydd y Cyngor yn adolygu a datblygu ein mesurau amddiffyn Seibrgadernid yn barhaus er mwyn mynd i'r afael â'r risgiau a wynebir gan ein gwasanaethau o ystyried y ddibyniaeth ar seilwaith a systemau TG.

Mae hyn yn cynnwys datblygu dull cydlynol ac wedi'i theilwra i risgiau a bygythiadau y gallem eu hwynebu a lliniaru diamddiffynedd posibl.

Camau Gweithredu:

Rheoli Risg

- Llunio a chynnal fframwaith rheoli risg, rheolaeth fewnol a llywodraethu ar gyfer atal a chanfod anghysonderau a thwyll.
- Prosesau, gweithdrefnau a rheolau i reoli newidiadau yn lefel bygythiad seibr a diamddiffynedd.

Rheoli Diamddiffynedd

- Rheoli elfennau diamddiffynedd newydd allai alluogi ymosodwr i gael mynediad i systemau critigol.
- Gweithredu rhaglen brofi hacio'r Cyngor; prosesau ymateb i ddigwyddiad seibr a Strategaeth Adfer o Drychineb.

Hyfforddiant ac Ymwybyddiaeth

- Sicrhau bod defnyddwyr TG y Cyngor yn ymwybodol o risgiau diweddaraf a'r camau priodol i'w cymryd.
- Ystyried gofynion hyfforddiant i swyddogion ac aelodau i gynnal lefelau o ymwybyddiaeth.

Cynllunio Ymateb i Ddigwyddiadau

- Cynnal cynllun ymateb a rheoli digwyddiad, gyda gweithredoedd, rolau a chyfrifoldebau clir.
- Paratoi Cynlluniau Ymateb i Drychineb i gynnwys rhestr o flaenoriaethau cytunedig o systemau i'w hadfer fel y cytunwyd gyda'r Uwch Dîm Arweinyddiaeth.
- Llunio cynllun cyfathrebu sydd yn cynnwys rhoi gwybod (er enghraifft) i'r corff goruchwylio perthnasol, uwch unigolion atebol, tîm cyfathrebu, WARP, Canolfan Seibrddiogelwch Genedlaethol, Llywodraeth Cymru a Swyddfa'r Comisiynydd Gwybodaeth neu'r heddlu fel y bo'n briodol (nid yw'n rhestr gyflawn) os bydd digwyddiad.
- Sicrhau bod Gwasanaethau yn cynnwys mesurau lliniaru mewn cynlluniau parhad i leihau amhariad o ganlyniad i ymosodiad seibr difrifol neu golli gwasanaethau TGCh yn ogystal ag ail-boblogi systemau gyda data a gollwyd neu nodyn a gofnodwyd o ganlyniad i unrhyw amhariad.

12. Mesur ein Seibrgadernid

Drwy gydol y cyfnod hwn o drawsnewid digidol, mae'r Cyngor wedi ymrwymo i ddarparu mesurau diogelwch gwybodaeth cadarn i ddiogelu data trigolion a budd-ddeiliaid rhag bygythiadau camddefnyddio a seibr, diogelu eu preifatrwydd drwy drefniadau rhannu data a llywodraethu gwybodaeth diogel a modern yn fewnol a chyda partneriaid.

Er mwyn parhau i ddarparu sicrwydd am effeithiolrwydd a chadernid trefniadau'r Cyngor ar gyfer diogelwch TG, bydd y Cyngor yn:

- Rheoli prosesau llywodraethu seibr ddiogelwch ac yn cynnal ardystiadau seibrgadernid allanol priodol.
- Sicrhau bod Seibrgadernid wedi'i gynnwys ar Fframwaith Rheoli Risg Gorfforaethol y Cyngor.
- Sicrhau bod polisïau/gweithdrefnau ar waith i adolygu gweithdrefnau mynediad y defnyddiwr.
- Sicrhau bod Gwasanaethau yn cynnal ymatebion seibr-benodol o fewn Cynlluniau Parhad Gwasanaeth.
- Cynnal cynllun ymateb a rheoli digwyddiad, gyda gweithredoedd, rolau a chyfrifoldebau clir, ynghyd â chynlluniau wedi'u paratoi ar gyfer blaenoriaethau adfer systemau. Bydd copi o bob digwyddiad yn cael ei recordio waeth beth yw'r angen i'w hadrodd.
- O fewn Cynllunio Adferiad wedi Trychineb TG - Sicrhau bod ymarferion profi'n cael eu cynnal yn erbyn y bygythiadau mwyaf tebygol a chynnal ymarferion adfer er mwyn sicrhau y gellir adfer systemau yn unol â blaenoriaethau y cytunwyd arnynt.
- Cynnal adolygiadau rheolaidd o systemau a seilwaith TGCh er mwyn sicrhau y ceir gwared ar fregusrwydd neu eu lliniaru.
- Adolygu rheoli gwerthwr - sicrhau bod gan Wasanaethau brosesau yn eu lle trwy gydol unrhyw gontract i asesu systemau seibrgadernid darparwyr trydydd parti. Fe ddylai hyn sicrhau bod yr holl ddata a systemau a gynhelir yn allanol yn cael eu diogelu'n briodol (gweler Atodiad 3).
- Parhau i edrych ar adnoddau amddiffyn seibr sy'n weithredol a thechnolegau newydd er mwyn sicrhau bod gan Gonwy y datrysiadau priodol i amddiffyn yn erbyn bygythiadau.
- Cynnal achrediadau a chydymffurfiaeth briodol er mwyn sicrhau bod ein mesurau seibrgadernid yn cael eu hadolygu'n allanol.
- Darparu hyfforddiant am amddiffyn gwybodaeth a diogelwch seibr perthnasol i staff ac aelodau etholedig.
- Mewn partneriaeth gyda Gwella a Datblygu Corfforaethol a Chynllunio Rhag Argyfwng, ystyried amserlen o ymarferion sy'n ymwneud â digwyddiadau seibr o fewn y cylch ehangach o ymarferion ymateb ac adfer sy'n ymwneud ag aml asiantaeth.
- Darparu mentrau ymwybyddiaeth seibrddiogelwch a hyfforddiant i ddinasyddion drwy lyfrgelloedd a ffynonellau eraill.

13. Rolau a Chyfrifoldebau Llywodraethu Seibrgadernid

Caiff llywodraethu seibrgadernid effeithiol yng Nghonwy ei ddarparu drwy'r rolau a swyddogaethau canlynol.

Rôl	Cyfrifoldebau
Y Cabinet	Mae'r Cabinet yn cynnwys Arweinydd y Cyngor ac uwch gynghorwyr eraill (Aelodau Cabinet). Bydd y Cabinet yn cytuno ac yn derbyn y newyddion diweddaraf am weithredu Strategaeth Seibrgadernid.
Tîm Arwain Strategol (TAS)	Mae TAS sy'n cynnwys Bwrdd Cyfarwyddwr y Cyngor yn noddi'r Strategaeth Seibrgadernid a goruchwylio fframwaith strategol. Drwy hwnnw y mae'r Cyngor yn llywodraethu ei adnoddau gwybodaeth.
Yr Uwch Dîm Arweinyddiaeth (UDA)	Mae'r UDA yn gyfrifol am sicrhau bod eu gwasanaethau wedi paratoi i ddelio gydag amhariad sylweddol neu golli gwasanaethau TG o fewn cynlluniau parhad gwasanaethau a sicrhau bod swyddogion yn ymwybodol o arferion da o ran amddiffyn gwybodaeth a chynnal seibrddiogelwch. Mae sicrhau bod cyflenwyr systemau yn darparu tystiolaeth o seibrgadernid effeithiol o ran eu gwasanaethau hefyd yn ystyriaeth allweddol. Cytuno ar gynllun blaenoriaethau ar gyfer adfer systemau a dyfeisiau os bydd cyfnod hir o amser pan na fydd pethau'n gweithio.
Yr Uwch Berchennog Risg Gwybodaeth	Mae'r Uwch Berchennog Risg Gwybodaeth yn gyfrifol am lywodraethu seibrddiogelwch a risg gwybodaeth o fewn y Cyngor. Mae hyn yn cynnwys sicrhau bod risg llywodraethu gwybodaeth yn cael ei reoli yn unol â GDPR. Serch hynny, er mai'r Uwch Berchennog Risg Gwybodaeth yw'r swyddog dynodedig, mae cyfrifoldeb am ddiogelu gwybodaeth a systemau yn cael ei rannu ar draws y sefydliad ac mae gan bob swyddog, partner ac aelod rôl i'w chwarae.
Pennaeth TG a Thrawsnewid Digidol	Y Gwasanaeth TG a Thrawsnewid Digidol sydd yn gwneud argymhellion a phenderfyniadau ynglŷn â goblygiadau technegol er mwyn sicrhau bod y Cyngor yn cadw lefelau effeithiol a phriodol o amddiffyniad seibrddiogelwch. Mae hyn yn cynnwys sicrhau bod goblygiadau seibrddiogelwch yn cael eu hadolygu a bod unrhyw newidiadau angenrheidiol yn cael eu hystyried yn iawn.
Grŵp Llywodraethu Gwybodaeth (GGG)	Mae'r GGG yn cynnwys uwch gynrychiolwyr o bob maes gwasanaeth. Mae'r grŵp yn gyfrifol am oruchwylio darparu Strategaeth Seibrgadernid a monitro ei effeithiolrwydd.
Bwrdd Digidol	Mae'r Bwrdd Digidol yn goruchwylio gweithredu Strategaeth Ddigidol Conwy. Maent yn sicrhau bod risgiau, materion a dibyniaethau yn cael eu rheoli'n rhagweithiol ac yn gwneud penderfyniadau mewn cysylltiad ag unrhyw risgiau a materion sydd wedi cael eu huwchgyfeirio mewn cysylltiad â'r rhaglen trawsnewid digidol.
Perchennog Asedau Gwybodaeth (PAG)	Mae Perchnogion Asedau Gwybodaeth yn gyfrifol am brosesu data personol o fewn eu maes busnes.

Rôl	Cyfrifoldebau
Aelodau a Swyddogion Cyngor Bwrdeistref Sirol Conwy	Cyfrifoldeb pob swyddog ac aelod yw cydymffurfio gyda'r safonau a osodir yn y Strategaeth Seibrgadernid.

14. Atodiad 1 – Safonau

Hanfodion Seibr

Mae Llywodraeth Cymru wedi gorfodi pob sefydliad sector cyhoeddus yng Nghymru i gymryd rhan yng nghynllun "Hanfodion Seibr a Mwy" Canolfan Seiberddiogelwch Genedlaethol fel dull o sicrhau bod amrywiaeth o fesurau amddiffyn ar waith. Mae Cyngor Bwrdeistref Sirol Conwy yn cymryd rhan yn y cynllun ac mae'n cael ei asesu'n flynyddol i wirio cydymffurfiaeth.

About Cyber Essentials - NCSC.GOV.UK

Cydymffurfiaeth â Rhwydwaith Sector Cyhoeddus

Er mwyn cael mynediad at rwydweithiau llywodraeth a rennir a sicrhau bod pob budd-ddeiliaid yn mabwysiadu safonau diogelwch priodol i leihau bygythiadau sy'n ymwneud â seibr, caiff y Cyngor ei asesu o leiaf unwaith bob dwy flynedd er mwyn sicrhau cydymffurfiaeth â safonau cytunedig. Mae ardystiad o gydymffurfiaeth yn helpu i sicrhau bod mesurau ar waith yn y Cyngor yn helpu i amddiffyn data, systemau a rhwydweithiau ehangach.

Cydymffurfio â Rhwydwaith Gwasanaethau Cyhoeddus - GOV.UK (www.gov.uk)

Safonau Diogelu Data'r Diwydiant Cardiau Talu (SDD DCT)

I gael sicrwydd am y mesurau diogelwch a fabwysiadir gan y Cyngor er mwyn sicrhau y cesglir taliadau'n ddiogel trwy gardiau talu, mae'r Cyngor hefyd yn cael ei adolygu'n flynyddol am gydymffurfiaeth â (SDD DCT).

Official PCI Security Standards Council Site - Verify PCI Compliance, Download Data Security and Credit Card Security Standards

BS EN ISO/IEC 27000:2020 Technoleg Gwybodaeth Technegau diogelwch. Systemau Rheoli Diogelwch Gwybodaeth.

Bydd y Cyngor hefyd yn gweithio i sicrhau bod mesurau seibrgadernid ar waith yn alinio â'r safonau a osodir yn nogfen Sefydliad Safonau Prydeinig sy'n nodi'r safonau ar gyfer seibrddiogelwch a diogelu data.

15. Atodiad 2 – NCSC: 10 Cam i Seibrddiogelwch

Trefn Rheoli Risg

Sefydlu trefn rheoli risg priodol ar ôl safonau ISO27k, ar draws y sefydliad.

Fe ddylai hyn gael ei gefnogi gan strwythur llywodraethu awdurdodedig, sydd yn cael ei gefnogi gan y bwrdd ac uwch reolwyr. Cyfathrebwch eich dull i reoli risg yn glir trwy ddatblygu polisïau ac arferion cymwys. Fe ddylai'r rhain anelu at sicrhau bod pob gweithiwr, contractwr a chyflenwr yn ymwybodol o'r dull, sut y gwneir penderfyniadau, ac unrhyw ffiniau risg cymwys.

Ffurfweddiad Diogel

Gall bod â dull i adnabod fersiynau a phrosesau technoleg gwaelodlin er mwyn rheoli ffurfweddiad wella diogelwch systemau'n fawr. Fe ddylech lunio strategaeth i gael gwared neu ddileu swyddogaeth ddiangen o systemau, a thrwsio diamddiffynedd yn sydyn, fel arfer drwy eu diweddaru. Mae methu â gwneud hynny yn debygol o arwain at risg gynyddol o beryglu systemau a gwybodaeth.

Diogelwch Rhwydwaith

Mae cysylltiadau o'ch rhwydweithiau i'r rhyngrwyd, a phartneriaid rhwydweithiau eraill, yn amlygu eich systemau a thechnolegau i ymosodiad. Drwy lunio a gweithredu polisïau syml ac ymatebion pensaernïol a thechnegol priodol, gallwch leihau'r cyfleoedd y bydd yr ymosodiadau yma'n llwyddo (neu'n achosi niwed i'ch sefydliad). Mae hi bron yn sicr fod rhwydweithiau eich safleoedd yn cyrraedd sawl safle ac yn defnyddio gweithio symudol neu o bell, a gwasanaethau cwmwl, gan olygu ei bopd hi'n anodd diffinio ffin rhwydwaith sefydlog. Yn hytrach na chanolbwyntio ar gysylltiadau corfforol yn unig, meddyliwch am ble mae'ch data'n cael ei storio a'i brosesu, a ble fyddai ymosodwr yn cael cyfle i amharu ag o.

Rheoli Breintiau Defnyddiwr

Os caiff defnyddwyr freintiau system neu hawliau mynediad data diangen, yna bydd effaith camddefnyddio neu beryglu cyfrif y defnyddiwr hwnnw yn fwy difrifol nag sydd angen iddo fo. Dylai pob defnyddiwr gael lefel rhesymol (ond minimol) o freintiau system a hawliau sydd eu hangen ar gyfer eu rôl. Dylai rhoi breintiau system uchel gael ei reoli'n ofalus. Cyfeirir at yr egwyddor yma fel 'braint lleiaf' (least privilege).

Addysg ac Ymwybyddiaeth Defnyddiwr

Mae gan ddefnyddwyr rôl allweddol i'w chwarae yn niogelwch eu sefydliad felly mae hi'n bwysig bod rheolau diogelwch a'r dechnoleg a ddarparwyd yn galluogi defnyddwyr i wneud eu gwaith yn ogystal â chadw'r sefydliad yn ddiogel. Gellir cefnogi hyn drwy ddarparu rhaglenni ymwybyddiaeth mewn modd systemig a hyfforddiant sydd yn darparu arbenigedd diogelwch yn ogystal â helpu i sefydlu diwylliant sydd yn ymwybodol o ddiogelwch.

Rheoli Digwyddiadau

Bydd pob sefydliad yn cael profiad o ddigwyddiadau diogelwch rhyw dro. Bydd buddsoddi mewn polisïau a phrosesau rheoli digwyddiadau effeithiol yn helpu i wella cadernid, cefnogi parhad busnes, gwella hyder cwsmeriaid a budd-ddeiliaid ac yn lleihau unrhyw effaith. Fe ddylech adnabod ffynonellau cydnabyddedig (mewnol neu allanol) o arbenigedd rheoli digwyddiad arbenigol

Atal Maleiswedd

Meddalwedd neu galedwedd maleiswedd, yw'r term cyffredinol i gynnwys unrhyw god neu gynnwys allai gael effaith maleisus, annymunol ar systemau. Daw rhywfaint o risg wrth gyfnewid unrhyw wybodaeth y gallai maleiswedd gael ei gyfnewid a allai effeithio'n ddifrifol ar eich systemau a gwasanaethau. Fe allai'r risg gael ei leihau drwy ddatblygu a gweithredu polisïau gwrth-faleiswedd priodol fel rhan o ddull 'amddiffyniad trylwyr' cyffredinol.

Monitro

Mae monitro system yn rhoi gallu i geisio canfod ymosodiadau gwirioneddol neu ymgais i ymosod ar systemau a gwasanaethau busnes. Mae monitro da yn hanfodol er mwyn ymateb yn effeithiol i ymosodiadau. Yn ychwanegol, mae monitro yn caniatáu i chi sicrhau bod systemau'n cael eu defnyddio'n briodol yn unol â pholisïau sefydliadol. Yn aml mae monitro yn allu allweddol sydd ei angen i gydymffurfio gyda gofynion cyfreithiol neu reoleiddiol.

Rheolau Cyfryngau Cludadwy

Mae cyfryngau cludadwy yn llwybr cyffredin i gyflwyno maleiswedd ac allgludo data sensitif yn ddamweiniol neu'n fwriadol. Fe ddylech chi fod yn glir am angen y busnes i ddefnyddio'r cyfryngau cludadwy a defnyddio rheolau diogelwch priodol i'w ddefnyddio.

Gweithio Gartref ac o Bell

Mae system gweithio'n symudol ac o bell yn cynnig llawer o fanteision, ond mae'n amlygu risgiau newydd sydd angen cael eu rheoli. Fe ddylech sefydlu polisïau a gweithdrefnau sy'n seiliedig ar risg sy'n cefnogi gweithio symudol neu fynediad o bell i systemau sydd yn briodol i ddefnyddwyr, yn ogystal â darparwyr gwasanaeth. Hyfforddi defnyddwyr am ddefnyddio eu dyfeisiau symudol yn ddiogel yn yr amgylcheddau y maent yn debygol o fod yn gweithio ynddynt.

16. Atodiad 3 – NCSC – Egwyddorion Diogelwch y Cwmwl.

Mae'r Ganolfan Seibrddiogelwch Genedlaethol yn darparu cyngor ac arweiniad ar ddewis platfform Cwmwl a Meddalwedd fel darparwyr gwasanaeth sydd yn bodoli anghenion diogelwch y Cyngor. Dylai Gwasanaethau ymgysylltu gyda/ceisio sicrwydd gan gyflenwyr cyn ymrwymo (ac yn ystod) unrhyw gontract bod eu system yn gadarn, yn ddiogel ac yn mabwysiadu rheolau seibrgadernid priodol.

Mae dolenni i dudalennau canllawiau Canolfan Seibrddiogelwch Genedlaethol ar gyfer dewis neu asesu darparwyr allanol wedi'u darparu isod.

Cloud Security Principles

Cloud Security Shared Responsibility Model

Lightweight Approach to Cloud Security (for Services NOT holding or processing sensitive data).

EGWYDDORION NCSC A ARGYMHELLIR AR GYFER DIOGELWCH Y CWMWL A CHWESTIYNAU AR GYFER DARPARWYR TRYDYDD PARTI
Egwyddor 1 – Amddiffyn Data wrth Drosglwyddo Pa fesurau y mae eich sefydliad yn eu mabwysiadu er mwyn diogelu data'n ddigonol yn erbyn ymyrryd a chlustfeinio wrth iddo drosglwyddo ar draws rhwydweithiau y tu mewn a thu allan i'r Cwmwl?
Egwyddor 2 – Amddiffyn a Chadernid Ased Sut mae'r data ac asedau sy'n eu storio neu eu prosesu yn cael eu hamddiffyn yn erbyn ymyrryd, colled, difrod neu atafaelu corfforol? Lle mae'r data'n cael ei gadw er mwyn sicrhau cydymffurfiaeth â deddfwriaeth diogelu data?
Egwyddor 3 – Gwahanu rhwng Cwsmeriaid Pa ffiniau diogelwch sydd ar waith er mwyn sicrhau na all cwsmeriaid eraill gael mynediad neu effeithio ar wasanaeth neu ddata Cyngor Bwrdeistref Sirol Conwy?
Egwyddor 4 – Fframwaith Llywodraethu Pa fframwaith llywodraethu diogelwch sydd ar waith er mwyn cydlynu a chyfarwyddo eich rheolaeth o'r gwasanaeth a gwybodaeth oddi mewn iddo.
Egwyddor 5 - Diogelwch Gweithredol Pa fesurau ydych chi'n eu defnyddio er mwyn sicrhau bod y gwasanaeth yn cael ei weithredu a'i reoli'n ddiogel er mwyn rhwystro, canfod neu atal ymosodiadau?
Egwyddor 6 - Diogelwch Personél Cadarnhewch os oes gan rhai o'ch personél fynediad i systemau a data'r Cyngor? Os mai dyma'r achos, nodwch fanylion sut rydych chi'n sicrhau dibynadwyedd staff, ac ymwybyddiaeth seibrddiogelwch a hyfforddiant llywodraethu Gwybodaeth neu ddiogelu data, mesurau technegol sydd ar gael sydd yn archwilio ac yn cyfyngu ar weithredoedd niweidiol posibl.
Egwyddor 7 – Datblygiad Diogel

Amlinellwch eich dull i ddylunio, datblygu a defnyddio eich system neu wasanaeth sydd yn lleihau a lliniaru yn erbyn bygythiadau i ddiogelwch neu argaeledd y system.
Egwyddor 8 – Diogelwch y Gadwyn Gyflenwi Pan fydd gan unrhyw drydydd parti fynediad at ddata cwsmeriaid neu'r gwasanaeth ar ran eich cwmni, darparwch fanylion sut y byddwch chi'n sicrhau bod y darparwyr hynny yn bodloni safonau diogelwch priodol i gynnal cadernid a diogelwch y system a data'r Cyngor?
Egwyddor 9 – Rheolaeth Ddiogel gan Ddefnyddiwr Ydi eich system yn cynnwys model mynediad sy'n galluogi'r Cyngor i weithredu rheolau mynediad ar sail rôl ar draws y gwasanaeth a data a gedwir ar y system? Sut y gellir rheoli mynediad i'r gwasanaeth yma'n ddiogel i atal mynediad diawdurdod a newid i adnoddau, rhaglenni neu ddata.
Egwyddor 10 – Adnabod a Dilysu Dywedwch sut mae pob mynediad i ryngwynebau gwasanaeth wedi'u cyfyngu i hunaniaeth dilys ac awdurdodedig diogel, allai berthyn i ddefnyddiwr sy'n unigolyn neu'n beiriant?
Egwyddor 11 – Amddiffyn Rhyngwyneb Allanol Eglurwch sut y caiff rhyngwynebau allanol neu rai nad ydych yn ymddiried ynddynt gymaint o'r gwasanaeth yn cael eu nodi a'u hamddiffyn yn briodol. Mae hyn yn cynnwys APIs, consolau ar y we a rhyngwynebau llinell gorchymyn.
Egwyddor 12 – Gweinyddu Gwasanaeth yn Ddiogel Nodwch fanylion sut mae dylunio, gweithredu a rheoli eich systemau gweinyddu yn dilyn arferion da mentergarwch, gan gydnabod eu gwerthu uchel i ymosodwyr.
Egwyddor 13 – Archwilio Gwybodaeth a Rhybuddio i Gwsmeriaid Nodwch wybodaeth ynglŷn â sut y byddai eich sefydliad yn adnabod digwyddiad diogelwch a pha ffynonellau gwybodaeth y byddech chi'n eu defnyddio i benderfynu sut a phryd y digwyddodd rhywbeth? Sut y byddwch chi'n darparu gwybodaeth archwilio neu rybuddion diogelwch pan gaiff ymdrechion i ymosod eu canfod?
Egwyddor 14 – Defnyddio Gwasanaeth yn Ddiogel Pa fesurau a chamau sydd ar waith er mwyn sicrhau bod y Cyngor yn bodloni ei gyfrifoldebau diogelu data? Ydi'r system neu wasanaeth sydd yn cael ei ddarparu yn ddiogel yn ôl dyluniad ac yn ddiofyn?