## **DIFROD MALEISUS A DAMWEINIOL**

**Difrod maleisus** yw pan gaiff data ei ddiwygio neu ei ddileu'n fwriadol.

**Colled ddamweiniol** yw pan gaiff data ei ddiwygio neu ei ddileu'n ddamweiniol.

**Enghraifft**

Banc ar-lein yw *Cymru Direct.* Gall cwsmeriaid weld cyfriflenni cyfoes a throsglwyddo arian rhwng eu cyfrifon gan ddefnyddio'r rhyngrwyd. Rhaid diogelu'r data hwn rhag *colled ddamweiniol* a *difrod maleisus*.

Gall colled ddamweiniol fod yn unrhyw un o'r canlynol:

* Cwsmer yn dileu gwybodaeth megis cyfriflenni
* Gweithwyr y banc yn dileu gwybodaeth yn ddamweiniol
* Gweinydd cyfrifiadurol yn chwalu/system yn methu
* Difrod i gyfrifiadur oherwydd tân/llifogydd
* Colli/ennill arian wrth drosglwyddo'n electronig

Gallai colled faleisus fod yn unrhyw un o'r canlynol:

* Gallai haciwr gyrchu data a'i newid/osod firws
* Gallai gweithwyr banc anfodlon ddifrodi data er mwyn gwneud drwg i'r banc
* Cwsmeriaid yn newid data amdanynt eu hunain neu gwsmeriaid eraill

**Copiau Wrth Gefn ac Adfer**

Mae pedair prif strategaeth y dylid eu dysgu er mwyn cael data wrth gefn ac adfer data. Y rhain yw:

|  |  |
| --- | --- |
| Strategaeth i sicrhau copïau wrth gefn | Strategaeth ar gyfer adfer data |
| • Tâp magnetig (gyriant)  • Disg caled yn cael ei gopïo i dâp bob nos/wythnos/mis | • Tâp yn cael ei gadw oddi ar y safle neu mewn sêff wrthdan  • Tâp yn gallu cael ei gopïo nôl i ddisg caled ar ôl methiant |
| • Gyriant caled symudadwy neu allanol  • Disg caled yn cael ei gopïo i'r disg caled allanol bob nos/wythnos/mis | • Disg caled allanol yn cael ei gadw oddi ar y safle neu mewn séff wrthdan  • Gall disg caled allanol gael ei gopïo yn ôl ar y disg caled gwreiddiol ar ôl methiant |
| • Defnyddio gweinydd ISP neu ddarparwr storfeydd trydydd parti drwy'r rhyngrwyd  • Caiff disg caled (newidiadau i ddisg) ei lanlwytho i ddarparwyr storfeydd trydydd parti bob nos/wythnos/mis | • Bydd y darparwr storfa trydydd parti oddi ar y safle  • Gall darparwr storfa trydydd parti lawrlwytho data nôl i ddisg caled y gweinydd newydd ar ôl methiant |
| • Defnyddio ail ddisg caled  • Caiff yr holl ddiwygiadau eu copïo i'r disg hwn. | • Lleolir y disg i ffwrdd o'r gweinydd  • Gall ail ddisg caled gael ei gopïo yn ôl i'r disg caled gwreiddiol ar ôl methiant. |

**Colli Data’n Ddamweiniol – Gwneud Copi Wrth Gefn o’r Data**

Mae gwneud copi wrth gefn o ddata'n golygu copïo'r data a'i gadw mewn lle diogel i ffwrdd o'r cyfrifiadur mewn lle diogel. Y ffordd fwyaf cyffredin o golli ffeil yw drwy wall dynol, lle mae person yn gwneud camgymeriad gydag un o'r gorchmynion neu gyfarwyddiadau ac yn dileu ffeil, neu gyfres gyfan o ffeiliau, nad oedd yn bwriadu eu dileu.

Ni ddylid byth cadw disgiau neu dapiau wrth gefn ger y cyfrifiadur oherwydd gall difrod i'r cyfrifiadur arwain at ddifrodi'r copi wrth gefn. Cyhyd ag y bo modd, dylid cadw copïau wrth gefn:

* Mewn séff wrthdan/wrthfom, a/neu
* Oddi ar y safle mewn lle gwahanol.

Mae gan systemau cyfrifiadurol mawr (gan gynnwys y rhwydwaith ysgol) weithdrefnau ar waith lle gwneir copi wrth gefn o ddata bob dydd (neu ddwywaith y dydd os yw'r data'n bwysig iawn ac yn newid yn aml yn ystod y diwrnod). Caiff tapiau wrth gefn eu cylchdroi fel arfer fel bod copïau'n cael eu cadw cyhyd â phosib cyn iddynt gael eu hailddefnyddio, ac mae hyn fel arfer yn golygu cael tapiau dyddiol, wythnosol a thymhorol.

Fel arfer, gwneir copïau wrth gefn o systemau mawr ar adeg pan nad yw'r system gyfrifiadurol yn brysur, er enghraifft, dros nos, fel nad yw'r broses yn arafu'r system.

### Disg yn Methu

Mae'n bwysig gwneud copi wrth gefn o ddata nid yn unig rhag ofn y caiff ei golli oherwydd tân a llifogydd, ond hefyd oherwydd y posibilrwydd y bydd y disg yn methu. Credir y bydd y rhan fwyaf o systemau cyfrifiadurol yn datblygu un diffyg difrifol yn ystod eu hoes.

Gyda disg caled nodweddiadol, yr amser cyfartalog rhwng bob methiant yw 20,000 i 200,000 o oriau. Mae hyn yn golygu os caiff cyfrifiadur ei ddefnyddio am 12 awr y dydd a 5 niwrnod yr wythnos a 52 wythnos y flwyddyn, yna byddech yn disgwyl i'w ddisg caled fethu unwaith mewn 6 blwyddyn! Os oedd y cyfrifiadur yn cael ei ddefnyddio fel gweinydd ffeil ar rwydwaith, bydd mwy na thebyg wedi'i droi ymlaen 24 awr y dydd a 365 niwrnod y flwyddyn, felly byddai'r ddisg caled yn methu bob 27 mis ar gyfartaledd.

Felly, mae sicrhau bod gennych gopïau wrth gefn o ddata yn hanfodol bwysig, yn enwedig lle mae busnes yn dibynnu'n drwm ar y system gyfrifiadurol a'i data, fel y mae mwyfwy o fusnesau yn ei wneud.

**Colli / Lladrata Data’n Fwriadol**

Mae llawer o'r data ar systemau cyfrifiadurol yn ddata personol, nid yn unig i'r cwmni sy'n ei storio, ond hefyd i'r gwrthrychau data y caiff data ei storio amdanynt. Felly, mae'n ofyniad yn ôl Deddf Diogelu Data 1998 bod data o'r fath yn cael ei ddiogelu'n iawn (gweler yn nes ymlaen). Gall sefydliad ddiogelu ei ddata rhag difrod a/neu ladrad bwriadol mewn nifer o ffyrdd.

**Diogelu Data**

Os caiff data ei drosglwyddo drwy rwydwaith, mae angen bod mesurau i sicrhau bod y data'n ddiogel. Os yw defnyddwyr yn anfon eu manylion cardiau credyd dros y rhyngrwyd, yna mae'n bwysig na all hacwyr gael mynediad iddynt.

Mae mesurau **diogeledd** yn cynnwys:

1. **Diogeledd Ffisegol.** Mae cyfyngu mynediad i gyfrifiaduron yn ffordd ddefnyddiol o sicrhau bod y data a ddelir arnynt yn cael ei gadw'n ddiogel. Yn amlwg, os nad oes gan berson fynediad i'r cyfrifiadur, nid oes unrhyw ffordd iddynt gyrchu'r data. Gallai diogeledd ffisegol olygu gosod clo ar ddrws y cyfarpar cyfrifiadurol neu gyfyngu ar nifer y mynedfeydd/allanfeydd a chael gwarchodwr, yn ogystal â dulliau mwy uwch-dechnolegol fel cloeon y gellir eu hagor drwy ddefnyddio rhif PIN yn unig, neu hyd yn oed dulliau mwy soffistigedig megis adnabyddiaeth llais neu ôl llaw gan ganiatáu mynediad i bersonél awdurdodedig.
2. **Amgryptio Data.** Gall ffeil sy'n cynnwys data arbennig o sensitif fod wedi'i amgryptio (h.y. wedi'i godio neu ei anhrefnu) ac felly, os bydd person heb awdurdod yn cyrchu'r data, yna mae'n annarllenadwy iddo nes bod ganddo'r côd i ddadgryptio'r data. Mae enghreifftiau o ffeiliau y gallant fod wedi'u hamgryptio yn cynnwys y ffeil o gyfrineiriau ar y rhwydwaith. Mae data'n cael ei amgryptio hefyd pan gaiff ei drosglwyddo dros rwydwaith i atal hacwyr rhag cyrchu data pwysig ar hyd cysylltiadau telegyfathrebu. Mae dylunwyr amgryptio wedi creu dulliau nad oes modd eu torri ar hyn o bryd mewn unrhyw amser rhesymol ac mae dulliau o'r math yn cael eu defnyddio gan fanciau a sefydliadau ariannol eraill wrth drosglwyddo arian yn electronig (EFT). Mae'r system hon yn trosglwyddo symiau mawr iawn o arian yn electronig ac felly mae'n rhaid ei diogelu drwy'r technegau amgryptio diweddaraf.
3. **Muriau Gwarchod.** Peiriant porth un pwrpas gyda rhagofalon diogeledd arbennig arno a ddefnyddir i fonitro rhwydwaith, yn enwedig cysylltiadau â'r rhyngrwyd. Y syniad yw diogelu segment o'r rhwydwaith a'i ffeiliau rhag hacwyr.

Mae blwch haearn yn amgylchedd arbennig a sefydlir i ddal haciwr sy'n mewngofnodi drwy gysylltiadau o bell. Gall gynnwys plisgyn wedi'i addasu sy'n cyfyngu ar symudiadau haciwr mewn ffyrdd nad ydynt yn amlwg, a ffeiliau 'abwyd' a luniwyd i gynnal ei ddiddordeb a'i gadw wedi'i fewngofnodi nes y gellir ei olrhain.

1. **Rheoli drwy Gyfrineiriau.** Mae cyfrineiriau'n ffordd gyffredin o ddiogelu data a chânt eu defnyddio mewn llawer o systemau lle mae'n rhaid diogelu data. Fodd bynnag, mae llwyddiant cyfrinair yn dibynnu'n fawr ar y cyfrinair a ddewisir gan y defnyddiwr ac a yw'n gallu ei gadw'n gyfrinach. Gall cyrchu ffeiliau gael ei reoli ar lefelau gwahanol gan gyfres o gyfrineiriau. Er enghraifft, efallai bydd gan glerc cofnodi data gyfrinair sy'n rhoi mynediad i rai cymwysiadau syml y mae eu hangen er mwyn iddo wneud ei waith, ond efallai bydd gan reolwr gyfrinair sy'n caniatáu iddo gyrchu cyfrifon y cwmni, etc. Dylai nifer y ceisiadau mewngofnodi gael eu rholi felly, er enghraifft, ar ôl 3 ymgais aflwyddiannus, dylai defnyddiwr gael ei gau allan a chofnod gael ei gadw o'r amser a natur yr ymgais. Gall hyn helpu defnyddwyr heb eu hawdurdodi sy'n ceisio dyfalu cyfrineiriau.

Mae **systemau biometrig** yn defnyddio nodweddion corfforol i adnabod defnyddiwr.

Cânt eu defnyddio yn y frwydr yn erbyn **dwyn hunaniaeth** lle mae person yn esgus bod yn rhywun arall er mwyn cyrchu deunydd anawdurdodedig.

Mae systemau biometrig, er nad ydynt yn ddi-feth, yn cynnig lefel uchel o ddiogeledd. Gyda'r rhan fwyaf, fodd bynnag, mae angen cyfarpar drud.

Dyma'r systemau biometrig sy'n cael eu defnyddio heddiw:

|  |  |  |
| --- | --- | --- |
| Sganiau retina | Caiff pelydryn is-goch pŵer isel ei daflu ar batrwm o bibellau gwaed yng nghefn y llygad.  Mae'n ddibynadwy iawn oherwydd nid oes gan unrhyw ddau berson yr un patrwm ar y retina.  C:\Users\Mr Thomas\Desktop\The Teacher Alevel only\theory\images\retina_scan.gif | |
| Sganio'r iris | Caiff patrwm yr iris yn y llygad ei sganio. | |
| Adnabod olion bysedd | Mae gan bob person ei ôl bys unigol ei hun.  Mae rhai gliniaduron yn cynnwys sganwyr olion bysedd sy'n dilysu defnyddiwr. | C:\Users\Mr Thomas\Desktop\The Teacher Alevel only\theory\images\fingerprint.gif |
| Adnabod wynebau | Gall siâp wyneb person gael ei sganio a'i gymharu â data sydd wedi'i storio. | C:\Users\Mr Thomas\Desktop\The Teacher Alevel only\theory\images\face_scan.gif |
| Adnabod lleisbrint | Adnabod person drwy ansawdd ei lais. | |

Mae systemau biometrig eraill yn cynnwys:

* **Adnabyddiaeth DNA**
* **Adnabyddiaeth Geometreg Llaw** - mae'n adnabod defnyddiwr drwy siâp ei law.
* **Adnabyddiaeth Gwythiennau'r Gledr** - mae'n adnabod defnyddwyr drwy'r patrwm o wythiennau yn eu cledrau.
* **Adnabod Llofnod**
* **Adnabyddiaeth Cerddediad Dynol** - y ffordd rydych chi'n cerdded!
* **Adnabyddiaeth Corn y Glust**
* **Adnabyddiaeth Arogl Corfforol**

**Firysau Cyfrifiadurol**

Mae **firws cyfrifiadurol** yn rhaglen a ddyluniwyd i greu niwsans i ddefnyddwyr eraill, neu'n fwy difrifol, i ddifrodi ffeiliau a storir ar gyfryngau magnetig i wahanol raddau. Yn gyffredinol, mae firws:

* Yn cael ei gyflwyno drwy gyfrwng megis disg hyblyg, yn enwedig y rhai sy'n storio meddalwedd dynwaredol neu raglenni rhanwedd; yn gallu heintio ffeiliau sy'n cael eu lawrlwytho o'r rhyngrwyd, a gall y firysau ledu ar draws systemau cyfrifiadurol;
* yn trosglwyddo'i hun o ddisg hyblyg sydd wedi'i heintio i gof y cyfrifiadur cyn gynted ag y defnyddir y cyfrwng;
* yn trosglwyddo o'r cof i'r ddyfais storio fewnol (megis y disg caled) ac yn aml yn cuddio'i hun yn y sector cychwyn lle gall heintio unrhyw ddisgiau hyblyg eraill a roddir yn y system gyfrifiadurol yn hawdd.

Mae rhai firysau'n niwsans yn unig, tra bydd eraill yn cael eu datblygu'n benodol i ddinistrio ffeiliau. Mae firysau'n fygythiad i ddata cyfrifiadurol, ac mae'n rhaid i reolwyr rhwydweithiau a chyfrifiaduron greu polisïau a fydd yn atal firysau rhag heintio'u systemau. Gellir cymryd nifer o fesurau i leihau'r perygl o firysau cyfrifiadurol:

1. Defnyddiwch feddalwedd berchnogol o ffynonellau dibynadwy'n unig.
2. Defnyddiwch ddisgiau wedi'u diogelu rhag ysgrifennu sy'n cael eu defnyddio i gyrchu data'n unig ac nid i newid y data. Bydd hyn yn atal y firws rhag cael ei ysgrifennu ar y disg heb i chi wybod hynny.
3. Defnyddiwch feddalwedd canfod firysau, er bod hyn yn effeithiol gyda firysau sy'n hysbys yn unig.
4. Defnyddiwch orsafoedd gwaith di-ddisg/cloeon disgiau hyblyg ar rwydweithiau.
5. Rheolwch y defnydd o ddisgiau hyblyg yn eich systemau cyfrifiadurol a gwaharddwch weithwyr rhag defnyddio'u disgiau hyblyg eu hunain ar system gyfrifiadurol y sefydliad.
6. Rheolwch/cyfyngwch ar fynediad i'r rhyngrwyd a gwaharddwch weithwyr rhag lawrlwytho ffeiliau heb ganiatâd ymlaen llaw.

**Cynllunio ar Gyfer Trychineb**

Bydd trychinebau **yn** digwydd.

Mae trychinebau'n cynnwys:

* **tân, llifogydd, mellt, corwyntoedd, bomiau** etc.
* methiant **caledwedd** - e.e. pen gyriant caled yn chwalu
* methiant **meddalwedd** - problemau adnoddau neu fygiau yn y system
* **fandaliaeth/hacio** bwriadol gan gynnwys firysau
* newid data'n **ddamweiniol** e.e. gan weithwyr dibrofiad
* gall **rhwydweithiau** fethu gan atal cyfathrebu.

Mae angen i gwmnïau wneud yn siŵr bod gweithdrefnau adfer yn dilyn trychineb digonol yn eu systemau cyfrifiadurol.

Mae tri cham i **gynlluniau trychineb -**

|  |  |
| --- | --- |
| Cyn | * dadansoddi risgiau, * mesurau ataliol * hyfforddi staff. |
| Yn ystod | * sut dylai staff ymateb pan fydd trychineb. |
| Wedyn | * mesurau adfer |

Gellir prynu **caledwedd** newydd yn lle'r galedwedd a ddifethwyd (er y bydd hyn efallai'n ddrud!).

Gellir ailosod **meddalwedd** (neu ei dadfygio gan yr adran raglenni).

Y broblem wirioneddol yw'r **data**. Ni all unrhyw fusnes fforddio colli ei ddata.

Dylid gwneud **copïau wrth gefn** o'r holl ddata'n rheolaidd. Mae hyn yn golygu mai'r sefyllfa waethaf yw y byddai'n rhaid i'r busnes fynd yn ôl i'r adeg y gwnaed y copïau wrth gefn diwethaf, a mynd ymlaen o'r pwynt hwnnw. Gall gwneud copïau wrth gefn gymryd amser hir gan ddibynnu ar y dull a ddefnyddir. Gweler adrannau blaenorol ar ddulliau cyfoes o wneud copïau wrth gefn, gan gynnwys defnyddio'r cwmwl.

Gellir trefnu systemau cyfathrebu eraill rhag ofn y bydd rhwydwaith yn methu.

**Cwestiwn 1**

Trafodwch fanteision biometreg ar gyfer gwella diogelwch, a thrafodwch unrhyw

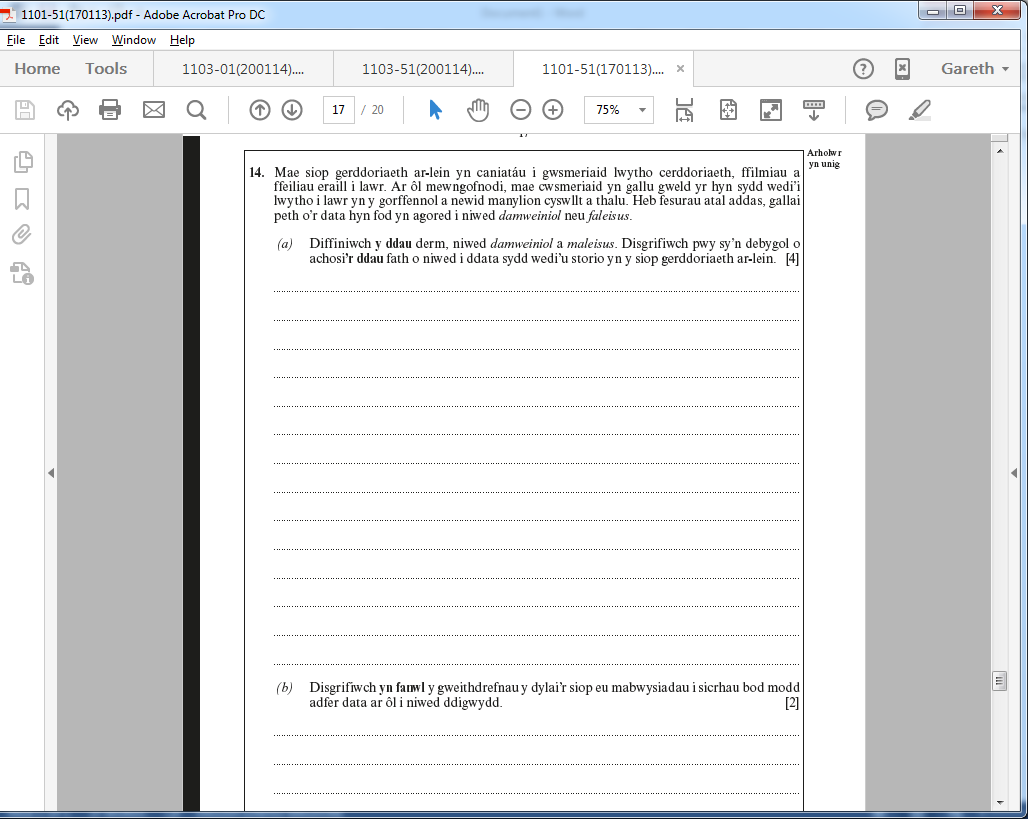
bryderon allai fod gan bobl am eu defnyddio. [5 marc]

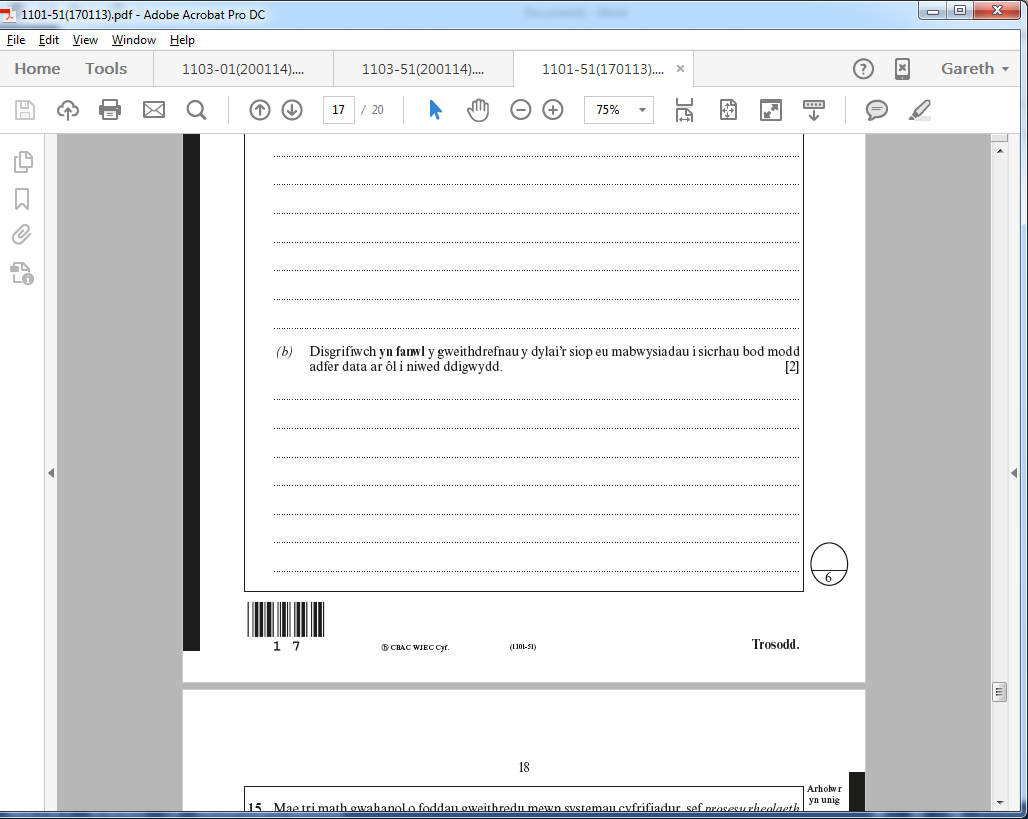
***(CG 3 - Ionawr 2014)***

**Cwestiwn 2**

Mae *Tywi* yn adwerthwr ar-lein mawr sy’n gwerthu llyfrau a gemau cyfrifiadur. Mae *Tywi* yn cynnal *cynllunio am drychineb* ar gyfer ei systemau cyfrifiadur. Trafodwch bwysigrwydd cynllunio am drychineb a disgrifiwch sut byddai cynllunio effeithiol am drychineb yn caniatáu i *Tywi* adfer yn gyflym yn dilyn trychineb.

***(CG 3 - Ionawr 2013)***

**Cwestiwn 3**



***(CG1 – Ionawr 2013)***