National Cyber Security Centre
a part of GCHQ

CYBER ESSENTIALS

Cyber Essentials:

Gofynion ar gyfer seilwaith TG

Fersiwn 3
Tachwedd 2021

Cynnwys

Beth sy'n newydd 4

Diffiniadau 5

Cwmpas 6

Trosolwg o'r cwmpas 6

Dod â'ch dyfais eich hun (BYOD) 7

Gweithio gartref 8

Dyfeisiau di-wifr 8

Gwasanaethau a reolir yn allanol — cwmwl 8

Gwasanaethau a reolir yn allanol — arall 10

Cymwysiadau gwe 10

Gofynion, yn ôl thema rheolaeth dechnegol 10

Waliau tân 10

Amcan 10

Cyflwyniad 10

Gofynion o dan y thema rheolaeth dechnegol hon 11

Ffurfweddiad diogel 12

Amcan 12

Cyflwyniad 12

Gofynion o dan y thema rheolaeth dechnegol hon 13

Rheoli mynediad defnyddwyr 14

Amcan 14

Cyflwyniad 14

Gofynion o dan y thema rheolaeth dechnegol hon 15

Diogelwch rhag maleiswedd 17

Amcan 18

Cyflwyniad 18

Gofynion o dan y thema rheolaeth dechnegol hon 18

Rheoli diweddariadau diogelwch 19

Amcan 20

Cyflwyniad..... 20
Gofynion o dan y thema rheolaeth dechnegol hon..... 20
Canllawiau Pellach..... 22
Gwneud copi wrth gefn o'ch data.....22

Nodwn y gofynion o dan bum thema rheolaeth dechnegol:

- waliau tân
- ffurfweddiad diogel
- rheoli mynediad defnyddwyr
- diogelwch rhag maleiswedd
- rheoli diweddariadau diogelwch

Fel ymgeisydd ar gyfer cynllun Cyber Essentials, rhaid i chi sicrhau bod eich sefydliad yn bodloni'r holl ofynion. Gall fod angen i chi ddarparu mathau gwahanol o dystiolaeth hefyd cyn y gall eich dewis Gorff Ardystio ddyfarnu ardystiad ar y lefel a geisir gennych.

Ewch ati i wneud y canlynol:

1. Pennu **ffin cwmpas** ar gyfer eich sefydliad a **nodi'r hyn a gwmpesir o fewn y ffin hon**.
2. Adolygu pob un o'r pum **thema rheolaeth dechnegol** a'r **rheolaethau a ymgorfforir ganddynt fel gofynion**.
3. Cymryd camau fel y bo angen i **sicrhau bod eich sefydliad yn bodloni pob gofyniad**, ym mhob rhan o'r cwmpas a bennwyd gennych.

Beth sy'n newydd

- Wedi ychwanegu gofyniad gweithio gartref a gwybodaeth am sut y dylid cynnwys y gofyniad hwn yn y cwmpas ardystiadau.
- Mae pob gwasanaeth cwmwl o fewn y cwmpas erbyn hyn, a cheir diffiniadau ychwanegol a thabl cyfrifoldeb a rennir er mwyn helpu gyda hyn.
- Wedi ymestyn y gofyniad dilysu aml-ffactor mewn perthynas â gwasanaethau cwmwl.
- Wedi diweddaru'r gofyniad dilysu seiliedig ar gyfrinair ac wedi ychwanegu adran newydd ar ddilysu aml-ffactor. Mae'r gofyniad hwn wedi cael ei symud i'r rheolaeth ‘mynediad defnyddwyr’ hefyd.
- Mae cleientiaid tenau o fewn y cwmpas erbyn hyn ac maent wedi cael eu hychwanegu at y diffiniad o ‘ddyfeisiau’.
- Wedi ychwanegu gofyniad newydd i ddatgloi dyfeisiau at y rheolaeth ‘ffurfweddiad diogel’.

- Wedi ychwanegu datganiad newydd sy'n egluro pam mae dyfeisiau defnyddwyr wedi cael eu cynnwys yn y cwmpas ardystiadau.
- Gwybodaeth bellach am gymwysiadau nas cefnogir wedi'i hychwanegu at y rheolaeth ‘rheoli diweddariadau diogelwch’.
- Wedi dileu ‘gweinyddion e-bost, gwe a chymwysiadau’ penodol o'r diffiniadau o reolaethau ac wedi rhoi ‘gweinyddion’ yn eu lle.
- Wedi diweddaru'r adran ‘dod â'ch dyfais eich hun’.
- Wedi diweddaru'r adran ‘dyfeisiadau di-wifr’.
- Wedi ychwanegu diffiniad newydd o ‘gweinyddion’.
- Wedi ychwanegu diffiniad newydd o ‘is-set’ a gwybodaeth am ei heffaith ar y cwmpas.
- Wedi ychwanegu diffiniad newydd o ‘trwyddedig a gefnogir’.

Diffiniadau

- Mae **meddalwedd** yn cynnwys systemau gweithredu, cymwysiadau masnachol parod, ategion, dehonglwyr, sgriptiau, llyfrgelloedd, meddalwedd rhwydwaith a chadarnwedd.
- Mae **dyfeisiau** yn cynnwys pob math o westeiwyr, cyfarpar rhwydweithio, gweinyddion, rhwydweithiau a dyfeisiau defnyddwyr megis cyfrifiaduron bwrdd gwaith, gliniaduron, cleientiaid tenau, llechi a ffonau symudol (ffonau clyfar) – p'un a ydynt yn rhai ffisegol neu'n rhai rhithwir.
- Mae **ymgeisydd** yn golygu'r sefydliad sy'n ceisio'r ardystiad, neu weithiau yr unigolyn sy'n gweithredu fel y prif bwynt cyswllt, yn dibynnu ar y cyd-destun.
- Datrysiad Rhwydwaith Preifat Rhithwir yw **VPN corfforaethol** sy'n cysylltu'n ôl â lleoliad swyddfa'r ymgeisydd neu wal dân rithwir/cwmwl. Rhaid iddo gael ei weinyddu gan y sefydliad sy'n gwneud cais er mwyn iddo allu defnyddio rheolaethau'r wal dân.
- Mae **data sefydliadol** yn cynnwys unrhyw ddata electronig sy'n eiddo i'r sefydliad sy'n gwneud cais. Er enghraifft, negeseuon e-bost, dogfennau swyddfa, data cronfa ddata, data ariannol.

- Mae **gwasanaeth sefydliadol** yn cynnwys unrhyw gymwysiadau meddalwedd, cymwysiadau cwmwl, gwasanaethau cwmwl, byrddau gwaith rhyngweithiol defnyddwyr a datrysiadau rheoli dyfeisiau symudol sy'n eiddo i'r sefydliad sy'n gwneud cais neu y mae'r sefydliad hwnnw wedi tanysgrifio iddynt. Er enghraifft: cymwysiadau gwe, Microsoft Office 365, Google Workspace, cynwysyddion rheoli dyfeisiadau symudol, Citrix Desktop, datrysiadau byrddau desg rhithwir, teleffoni IP.
- Ystyr **is-set** yw rhan o'r sefydliad y mae ei rhwydwaith wedi'i wahanu oddi wrth weddill y sefydliad gan wal dân neu VLAN.
- Ystyr **gweinyddion** yw dyfeisiadau penodol sy'n darparu data neu wasanaethau sefydliadol i ddyfeisiau eraill fel rhan o fusnes yr ymgeisydd.
- Ystyr **meddalwedd trwyddedig a gefnogir** yw meddalwedd y mae gennych hawl gyfreithiol i'w defnyddio ac y mae gwerthwr wedi ymrwymo i'w chefnogi drwy ddarparu diweddariadau rheolaidd (patsys). Rhaid i'r gwerthwr nodi'r dyddiad y bydd y diweddariadau yn dod i ben. Nid oes rhaid i'r gwerthwr fod yn gyfrifol am greu'r fersiwn wreiddiol o'r feddalwedd, ond rhaid ei fod yn gallu addasu'r feddalwedd wreiddiol i greu diweddariadau.

Cwmpas

Trosolwg o'r cwmpas

Dylai gweithgarwch asesu ac ardystio gwmpasu'r holl seilwaith TG a ddefnyddir i gyflawni busnes yr ymgeisydd neu, os bydd angen, is-set a ddiffinnir yn dda ac a gaiff ei rheoli ar wahân. Y naill ffordd neu'r llall, rhaid i ffin y cwmpas gael ei diffinio'n glir o ran yr uned fusnes sy'n ei rheoli, ffin y rhwydwaith a'r lleoliad ffisegol. Rhaid i'r ymgeisydd a'r Corff Ardystio gytuno ar y cwmpas cyn i'r asesiad ddechrau.

Gellir defnyddio is-set i ddiffinio'r hyn **sydd o fewn y cwmpas** neu **y tu allan i'r cwmpas** ar gyfer Cyber Essentials.

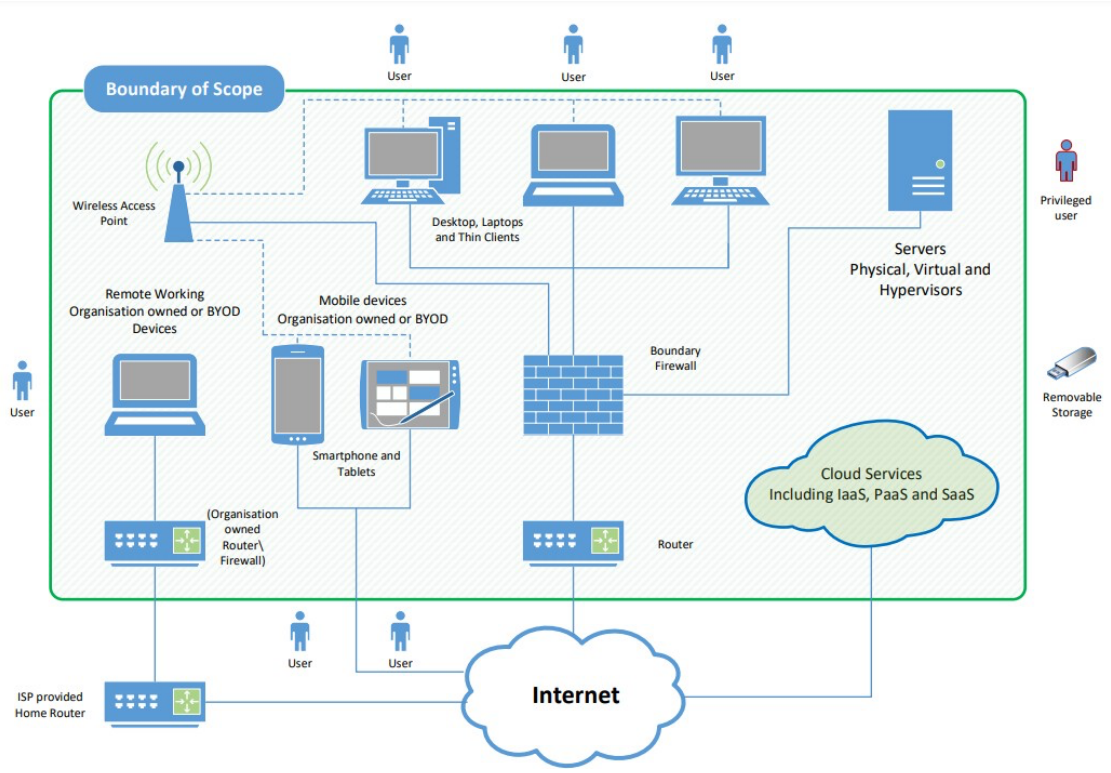
> **Gwybodaeth** Sefydliadau sy'n dewis cwmpas sy'n cynnwys y seilwaith TG gyfan sy'n cael eu diogelu orau. Maent hefyd yn cynyddu hyder cwsmeriaid.

Mae'r gofynion yn gymwys i'r holl ddyfeisiau a meddalwedd sydd o fewn ffin y cwmpas ac sy'n bodloni unrhyw rai o'r amodau hyn:

- gallant dderbyn cysylltiadau rhwydwaith gan westeiwyr annibynadwy a gysylltir â'r rhyngrwyd; neu
- gallant sefydlu cysylltiadau a gychwynnir gan ddefnyddwyr a anfonir i ddyfeisiau drwy'r rhyngrwyd; neu
- gallant reoli'r llif data rhwng unrhyw rai o'r dyfeisiau uchod a'r rhyngrwyd.

Mae cwmpas nad yw'n cynnwys dyfeisiau defnyddwyr yn annerbyniol.

Ffigur 1: Cwmpas y gofynion ar gyfer seilwaith TG –



Dod â'ch dyfais eich hun (BYOD)

Yn ogystal â dyfeisiau symudol neu ddyfeisiau a weithredir o bell sy'n eiddo i'r sefydliad, mae dyfeisiau sy'n eiddo i ddefnyddwyr sy'n cyrchu data neu wasanaethau sefydliadol (fel y diffinnir uchod) o fewn y **cwmpas**. Fodd bynnag, mae unrhyw ddyfais symudol neu ddyfais a weithredir o bell a ddefnyddir at y dibenion canlynol **yn unig**:

- cymwysiadau llais cynhenid
- cymwysiadau testun cynhenid
- cymwysiadau dilysu aml-ffactor

y tu allan i'r cwmpas.

Yn draddodiadol, câi dyfeisiau defnyddwyr eu rheoli drwy system weinyddol ganolog a oedd yn sicrhau cysondeb ledled y sefydliad. Yn y cyfryw achosion, mae'r broses o ardystio'r rheolaethau diogelwch yn un syml gan y bydd gwneuthuriad neu gyfeirnod safonol i'w asesu.

Mae BYOD yn cymhlethu pethau, gan fod defnyddwyr yn cael mwy o ryddid i ‘bersonoli’ eu profiad, sy'n golygu ei bod hi'n fwy heriol rhoi'r rheolaethau ar waith mewn ffordd gyson. Dylai defnyddio'r diffiniadau o ddata a gwasanaethau sefydliadol i atgyfnerthu polisïau mynediad cryf ddileu rhywfaint o'r amwysedd hwn.

Gweithio gartref

Y dull diofyn yw bod pob dyfais gweithio gartref corfforaethol neu BYOD a ddefnyddir ar gyfer ymgymryd â busnes yr ymgeisydd yn y cartref **o fewn y cwmpas** ar gyfer Cyber Essentials.

Mae llwybryddion Darparwyr Gwasanaethau Rhyngrwyd (ISP) a llwybryddion a ddarperir gan ddefnyddwyr **y tu allan i'r cwmpas** sy'n golygu bod yn rhaid i reolaethau wal dân Cyber Essentials gael eu gosod ar ddyfeisiau'r defnyddiwr (e.e. wal dân meddalwedd).

Os bydd y sefydliad sy'n gwneud cais yn rhoi llwybrydd i'r sawl sy'n gweithio gartref, yna bydd y llwybrydd hwnnw **o fewn y cwmpas**.

Os yw'r sawl sy'n gweithio gartref yn defnyddio VPN corfforaethol, mae ffin ei rwydwaith ar wal dân y cwmni neu wal dân rithwir/cwmwl.

Dyfeisiau di-wifr

Mae dyfeisiau di-wifr (gan gynnwys pwyntiau mynediad di-wifr):

- **o fewn y cwmpas** os gallant gyfathrebu â dyfeisiau eraill drwy'r rhyngrwyd
- **nid ydynt o fewn y cwmpas** os nad yw'n bosibl i'r sawl sy'n ymosod wneud hynny yn uniongyrchol o'r rhyngrwyd (nid yw cynllun Cyber Essentials yn ymwneud ag ymosodiadau y gellir ond eu lansio o fewn amrediad signal y ddyfais ddi-wifr)
- **nid ydynt o fewn y cwmpas** os ydynt yn rhan o lwybrydd ISP yn y cartref

Gwasanaethau a reolir yn allanol – cwmwl

Os caiff data neu wasanaethau'r ymgeisydd eu lletya ar wasanaethau cwmwl, yna rhaid i'r gwasanaethau hyn fod **o fewn y cwmpas**.

O ran gwasanaethau cwmwl, **yr ymgeisydd sy'n gyfrifol bob amser** am sicrhau bod yr holl reolaethau yn cael eu rhoi ar waith, ond gall rhai o'r rheolaethau gael eu rhoi ar waith gan ddarparwr y gwasanaethau cwmwl. Y math o wasanaeth cwmwl fydd yn penderfynu pwy fydd yn rhoi pa reolaeth ar waith. Ystyriwn dri math gwahanol o wasanaeth cwmwl:

- **Seilwaith fel Gwasanaeth (IaaS)** – mae darparwr y gwasanaeth cwmwl yn darparu gweinyddion rhithwyr a chyfarpar rhwydwaith sy'n cael eu ffurfweddu a'u rheoli gan yr ymgeisydd, yn yr un ffordd ag y byddai'n digwydd gyda chyfarpar ffisegol. Ymhlith yr enghreifftiau o IaaS mae Rackspace, Google Compute Engine, neu Amazon EC2.
- **Llwyfan fel Gwasanaeth (PaaS)** – darparwr y gwasanaeth cwmwl sy'n darparu ac yn rheoli'r seilwaith sylfaenol, a'r ymgeisydd sy'n darparu ac yn rheoli'r cymwysiadau. Ymhlith yr enghreifftiau o PaaS mae Azure Web Apps ac Amazon Web Services Lambda.
- **Meddalwedd fel Gwasanaeth (SaaS)** – darparwr y gwasanaeth cwmwl sy'n darparu cymwysiadau i'r ymgeisydd, a'r ymgeisydd sy'n ffurfweddu'r gwasanaethau. Rhaid i'r ymgeisydd gymryd amser o hyd i sicrhau bod y gwasanaeth yn cael ei ffurfweddu'n ddiogel. Ymhlith yr enghreifftiau o SaaS mae Microsoft 365, Dropbox a Gmail.

Dyluniad y gwasanaeth cwmwl fydd yn penderfynu pwy fydd yn rhoi'r rheolaethau ar waith, ond mae'r tabl isod yn rhoi canllaw ar bwy y byddai disgwyl iddo roi pob rheolaeth ar waith fel arfer:

Gofyniad	**IaaS**	**PaaS**	**SaaS**
waliau tân	yr ymgeisydd a darparwr y gwasanaeth cwmwl	darparwr y gwasanaeth cwmwl a'r ymgeisydd weithiau hefyd	darparwr y gwasanaeth cwmwl
ffurfweddiad diogel	yr ymgeisydd a darparwr y gwasanaeth cwmwl	yr ymgeisydd a darparwr y gwasanaeth cwmwl	yr ymgeisydd a darparwr y gwasanaeth cwmwl
rheoli mynediad defnyddwyr	ymgeisydd	ymgeisydd	ymgeisydd
diogelwch rhag maleiswedd	yr ymgeisydd a darparwr y gwasanaeth cwmwl	darparwr y gwasanaeth cwmwl a'r ymgeisydd weithiau hefyd	darparwr y gwasanaeth cwmwl
rheoli diweddariadau diogelwch	yr ymgeisydd a darparwr y gwasanaeth cwmwl	yr ymgeisydd a darparwr y gwasanaeth cwmwl	darparwr y gwasanaeth cwmwl

Os bydd darparwr y gwasanaeth cwmwl yn rhoi rheolaeth ar waith, rhaid i'r ymgeisydd fodloni ei hun bod hyn wedi cael ei wneud drwy ymrwymiad a wnaed gan ddarparwr y gwasanaeth cwmwl i'w rhoi ar waith o fewn cymalau cytundebol neu ddogfennau y cyfeirir atynt mewn contract, fel datganiadau diogelwch neu ddatganiadau preifatrwydd. Yn aml, bydd darparwyr gwasanaethau cwmwl yn egluro sut maent yn rhoi mesurau diogelwch ar waith mewn dogfennau a gyhoeddir yn eu canolfannau ymddiriedaeth, a fydd yn cynnwys cyfeiriad at 'fodel cyfrifoldeb a rennir'.

Gwasanaethau a reolir yn allanol – arall

Os yw'r ymgeisydd yn defnyddio gwasanaethau eraill a reolir yn allanol (fel gweinyddiaeth o bell), efallai na fydd yn bosibl iddo fodloni'r holl ofynion yn uniongyrchol. Gall yr ymgeisydd **ddewis** a ddylai'r gwasanaethau hyn gael eu cynnwys o fewn ffin y cwmpas, yn ôl dichonoldeb.

Os cânt eu cynnwys, yna rhaid i'r ymgeisydd allu dangos bod y gofynion sydd y tu hwnt i reolaeth yr ymgeisydd yn cael eu bodloni'n ddigonol gan ddarparwr y gwasanaeth. Gellir ystyried tystiolaeth sy'n bodoli eisoes (megis tystiolaeth a ddarperir drwy ardystiad PCI ar gyfer gwasanaeth cwmwl, ac ardystiadau ISO 27001 sy'n cwmpasu cwmpas priodol).

Cymwysiadau gwe

Mae cymwysiadau gwe masnachol a grëir gan gwmnïau datblygu (yn hytrach na datblygwyr mewnol) ac sydd ar gael i'r cyhoedd drwy'r rhyngrwyd **o fewn y cwmpas** yn ddiofyn. **Nid yw** cydrannau pwrpasol a chydrannau sydd wedi'u teilwra ar gyfer cymwysiadau gwe **o fewn y cwmpas**. Y prif fesur lliniaru yn erbyn gwendidau yn y cyfryw gymwysiadau yw gwaith datblygu a phrofi cadarn yn unol ag arferion gorau masnachol, megis safonau'r Prosiect Diogelwch Cymwysiadau Gwe Agored (OWASP).

Gofynion, yn ôl thema rheolaeth dechnegol

Waliau tân

Yn gymwys i'r canlynol: waliau tân ffiniau, cyfrifiaduron bwrdd gwaith, gliniaduron, llwybryddion, gweinyddion, IaaS, PaaS, SaaS.

Amcan

Sicrhau mai dim ond gwasanaethau rhwydwaith diogel ac angenrheidiol y gellir cael mynediad atynt o'r rhyngrwyd.

Cyflwyniad

Mae pob dyfais yn rhedeg gwasanaethau rhwydwaith, sy'n creu rhyw fath o ddull cyfathrebu â dyfeisiau a gwasanaethau eraill. Drwy gyfyngu ar fynediad at y gwasanaethau hyn, rydych yn lleihau eich amlygiad i ymosodiadau. Gellir gwneud hyn drwy ddefnyddio waliau tân a dyfeisiau rhwydwaith cyfatebol, neu bolisïau llif data mewn gwasanaethau cwmwl.

Dyfais rhwydwaith yw wal dân ffiniau a all gyfyngu ar draffig rhwydwaith sydd ar y ffordd i mewn ac ar y ffordd allan i wasanaethau ar ei rhwydwaith o gyfrifiaduron a dyfeisiau symudol. Gall helpu i ddiogelu yn erbyn ymosodiadau seiber drwy roi cyfyngiadau, a elwir yn 'rheolau wal dân', ar waith, a all ganiatáu neu rwystro traffig yn ôl ei ffynhonnell, ei gyrchfan a'r math o brotocol cyfathrebu.

Fel arall, lle nad yw sefydliad yn rheoli'r rhwydwaith y mae dyfais wedi'i chysylltu ag ef, rhaid i wal dâl feddalwedd gael ei ffurfweddu ar ddyfais. Mae'r wal hon yn gweithio yn yr un ffordd â wal dân ffiniau ond dim ond y ddyfais unigol y mae wedi'i ffurfweddu arni y mae'n ei diogelu. Gall y dull hwn ddarparu ar gyfer rheolau wedi'u teilwra'n well ac mae'n golygu y bydd y rheolau yn gymwys i'r ddyfais lle bynnag y caiff ei defnyddio. Fodd bynnag, mae hyn yn cynyddu'r costau gweinyddol sy'n gysylltiedig â rheoli rheolau wal dân.

> **Gwybodaeth** Erbyn hyn, caiff wal dân meddalwedd ei gosod ar y rhan fwyaf o systemau gweithredu cyfrifiaduron bwrdd gwaith a gliniaduron, a chynghorwn y dylid troi'r wal hon ymlaen yn lle cymhwysiad wal dân trydydd parti.

Gofynion o dan y thema rheolaeth dechnegol hon

Rhaid i bob dyfais sydd o fewn y cwmpas gael ei diogelu gan wal dân sydd wedi'i ffurfweddu'n gywir (neu ddyfais rhwydwaith gyfatebol).

Ar gyfer pob wal dân (neu ddyfais rhwydwaith gyfatebol), rhaid i'r sefydliad sy'n gwneud cais wneud y canlynol fel mater o drefn:

- disodli unrhyw gyfrinair gweinyddol diofyn â chyfrinair arall sy'n anodd ei ddyfalu (gweler dilysu seiliedig ar gyfrinair) – neu analluogi mynediad gweinyddol o bell yn gyfan gwbl
- atal mynediad i'r rhyngwyneb gweinyddol (a ddefnyddir i reoli ffurfweddiad wal dân) o'r rhyngrwyd, oni fydd angen busnes clir wedi'i ddogfennu a bod y rhyngwyneb yn cael ei ddiogelu gan un o'r rheolaethau canlynol:
    - dilysu aml-ffactor (gweler y manylion isod)

    - rhestr caniatáu IP sy'n cyfyngu ar fynediad at ystod fach o gyfeiriadau dibynadwy ar y cyd â dull dilysu cyfrineiriau a reolir yn gywir

- rhwystro cysylltiadau heb eu dilysu sydd ar y ffordd i mewn yn ddiofyn
- sicrhau bod rheolau wal dân sydd ar y ffordd i mewn yn cael eu cymeradwyo a'u dogfennu gan unigolyn awdurdodedig; rhaid i'r angen busnes gael ei gynnwys yn y ddogfennaeth
- dileu neu analluogi rheolau wal dân diangen yn gyflym, os nad oes angen eu hangen mwyach
- defnyddio wal dân meddalwedd ar ddyfeisiau a ddefnyddir ar rwydweithiau annibynadwy, megis mannau poblogaidd lle y gall y cyhoedd ddefnyddio Wi-Fi

Ffurfweddiad diogel

Yn gymwys i'r canlynol: gweinyddion, cyfrifiaduron bwrdd gwaith, gliniaduron, llechi, ffonau symudol, cleientiaid tenau, IaaS, PaaS, SaaS.

Amcan

Sicrhau bod cyfrifiaduron a dyfeisiau rhwydwaith yn cael eu ffurfweddu'n gywir er mwyn:

- lleihau lefel y gwendidau cynhenid
- darparu'r gwasanaethau sydd eu hangen i gyflawni eu rôl yn unig

Cyflwyniad

Nid yw cyfrifiaduron a dyfeisiau rhwydwaith bob amser yn ddiogel yn eu ffurfweddiadau diofyn. Yn aml, mae ffurfweddiadau safonol, parod yn cynnwys un neu fwy o fannau gwan megis:

- cyfrif gweinyddol â chyfrinair diofyn a bennwyd ymlaen llaw ac sy'n hysbys i'r cyhoedd neu ddilysiad aml-ffactor sydd heb ei alluogi
- cyfrifon defnyddwyr diangen a alluogwyd ymlaen llaw (weithiau gyda breintiau mynediad arbennig)
- cymwysiadau neu wasanaethau diangen a osodwyd ymlaen llaw

Gall gosodiadau diofyn ar gyfrifiaduron a dyfeisiau rhwydwaith roi amrywiaeth o gyfleoedd i'r rhai sy'n cyflawni ymosodiadau seiber gael mynediad heb awdurdod at wybodaeth sensitif sefydliad – a hynny'n aml yn rhwydd.

Drwy ddefnyddio rhai rheolaethau technegol syml wrth osod cyfrifiaduron a dyfeisiau rhwydwaith, gallwch leihau gwendidau cynhenid a sicrhau gwell diogelwch yn erbyn mathau cyffredin o ymosodiadau seiber.

Gofynion o dan y thema rheolaeth dechnegol hon

Cyfrifiaduron a dyfeisiau rhwydwaith

Rhaid bod yr ymgeisydd yn mynd ati'n weithredol i reoli cyfrifiaduron a dyfeisiau rhwydwaith. Rhaid iddo wneud y canlynol fel mater o drefn:

- dileu ac analluogi cyfrifon defnyddwyr diangen (fel cyfrifon gwesteion a chyfrifon gweinyddol na chânt eu defnyddio)
- newid unrhyw gyfrineiriau diofyn neu gyfrineiriau y gellir eu dyfalu ar gyfer cyfrifon (gweler dilysu seiliedig ar gyfrinair)
- dileu neu analluogi meddalwedd ddiangen (gan gynnwys cymwysiadau, cyfleustodau system a gwasanaethau rhwydwaith)
- analluogi unrhyw nodwedd *auto-run* sy'n caniatáu gweithredu ffeil heb awdurdod defnyddiwr (megis pan gaiff ei lawrlwytho o'r rhyngrwyd)
- sicrhau bod defnyddwyr wedi'u dilysu cyn caniatáu mynediad at ddata neu wasanaethau sefydliadol
- sicrhau rheolaethau datgloi dyfeisiau priodol (gweler ‘datgloi dyfeisiau’, isod) ar gyfer defnyddwyr sy'n bresennol yn gorfforol.

Manylion datgloi dyfeisiau

Pan fydd angen i ddefnyddiwr fod yn bresennol yn gorfforol er mwyn cael mynediad at y gwasanaethau y mae dyfais yn eu cynnig (e.e. mewngofnodi i liniadur, datgloi ffôn symudol), rhaid i'r defnyddiwr ddatgloi'r ddyfais gan ddefnyddio manylion megis gwybodaeth fiometrig, cyfrinair neu PIN cyn cael mynediad at y gwasanaethau.

Rhaid i wybodaeth (?) fiometrig, cyfrineiriau a manylion PIN gael eu diogelu rhag ymosodiad nerth bôn braich gan o leiaf un o'r canlynol:

- arafu nifer yr ymgeisiau *(throttling)*. Mae hyn yn golygu bod yr amser y mae'n rhaid i ddefnyddiwr aros rhwng pob ymgais yn cynyddu gyda phob ymgais aflwyddiannus. Dylai hyn ganiatáu 10 o gynigion ar y mwyaf mewn 5 munud.
- cloi dyfeisiau ar ôl 10 ymgais aflwyddiannus ar y mwyaf

Rhaid i reolaethau technegol gael eu defnyddio i reoli ansawdd y manylion. Os mai dim ond ar gyfer datgloi dyfais y mae angen y manylion, rhaid defnyddio cyfrinair neu PIN sy'n cynnwys o leiaf 6 nod.

Pan ddefnyddir y manylion datgloi dyfeisiau mewn mannau eraill, rhaid i'r gofynion cyfrinair llawn yn ‘rheoli mynediad defnyddwyr’ gael eu cymhwyso at y manylion.

Rheoli mynediad defnyddwyr

Yn gymwys i'r canlynol: gweinyddion, cyfrifiaduron bwrdd gwaith, gliniaduron, llechi, ffonau symudol, IaaS, PaaS, SaaS.

Amcan

Sicrhau bod cyfrifon defnyddwyr:

- yn cael eu neilltuo i unigolion awdurdodedig yn unig
- dim ond yn rhoi mynediad at y cymwysiadau, y cyfrifiaduron a'r rhwydweithiau hynny sydd eu hangen ar y defnyddiwr i gyflawni ei rôl

Cyflwyniad

Mae pob cyfrif defnyddiwr gweithredol yn eich sefydliad yn hwyluso mynediad at ddyfeisiau a chymwysiadau a gwybodaeth fusnes sensitif. Drwy sicrhau mai dim ond unigolion awdurdodedig sydd â chyfrifon defnyddwyr, ac mai dim ond mynediad at yr hyn sydd ei angen arnynt i gyflawni ei rôl sydd ganddynt, rydych yn lleihau'r risg y caiff gwybodaeth ei dwyn neu ei difrodi.

O gymharu â chyfrifon defnyddwyr arferol, mae gan gyfrifon â breintiau mynediad arbennig fynediad ychwanegol at wybodaeth, dyfeisiau a chymwysiadau. Pan gaiff y cyfryw gyfrifon eu peryglu, gellir manteisio ar y rhyddid ychwanegol a gynigir ganddynt i lygru gwybodaeth ar raddfa fawr, aflonyddu ar brosesau busnes a chael mynediad heb awdurdod at ddyfeisiau eraill yn y sefydliad.

Er enghraifft, mae ‘cyfrifon gweinyddol’ yn enwedig yn cynnwys llawer o freintiau. Fel arfer, mae'r cyfryw gyfrifon yn caniatáu'r canlynol:

- gweithredu meddalwedd sy'n gallu gwneud newidiadau sylweddol i'r system weithredu sy'n berthnasol i ddiogelwch
- newidiadau i'r system weithredu ar gyfer rhai defnyddwyr neu bob defnyddiwr
- creu cyfrifon newydd a dyrannu'r breintiau sy'n gysylltiedig â nhw

Bydd gan bob math o weinyddwr gyfrifon o'r fath, gan gynnwys gweinyddwyr pyrth a gweinyddwyr lleol.

Nawr ystyriwch, os bydd defnyddiwr yn agor URL neu atodiad e-bost maleisus, fel arfer bydd gan unrhyw faleiswedd gysylltiedig lefel braint y cyfrif y mae'r defnyddiwr hwnnw yn ei ddefnyddio ar y pryd. Yn amlwg, rhaid bod yn ofalus iawn wrth neilltuo a defnyddio cyfrifon brientiedig.

Enghraifft

> Mae Jody wedi mewngofnodi i gyfrif gweinyddol. Os bydd Jody yn agor URL neu atodiad e-bost maleisus, mae'n debygol y bydd unrhyw faleiswedd gysylltiedig yn caffael breintiau gweinyddol. Yn anffodus, dyna'n union sy'n digwydd. Gan ddefnyddio breintiau gweinyddol Jody, mae math o faleiswedd o'r enw meddalwedd wystlo yn amgryptio'r holl ddata ar y rhwydwaith ac yna'n mynnu pridwerth. Roedd y feddalwedd wystlo yn gallu amgryptio llawer mwy o ddata nag a fyddai wedi bod yn bosibl gyda breintiau defnyddwyr safonol, gan wneud y broblem yn un llawer mwy difrifol.

Gofynion o dan y thema rheolaeth dechnegol hon

Rhaid bod gan yr ymgeisydd reolaeth dros ei gyfrifon defnyddwyr a'r breintiau mynediad a roddir i bob cyfrif defnyddiwr sydd â mynediad at ddata a gwasanaethau'r sefydliad. Yn bwysig, mae hyn yn cynnwys cyfrifon y mae trydydd partïon yn eu defnyddio i gael mynediad, er enghraifft i reoli dyfeisiau neu wasanaethau cymorth. Rhaid iddo hefyd ddeall sut mae cyfrifon defnyddwyr yn dilysu ac yn rheoli cryfder y dull dilysu hwnnw. Mae hyn yn golygu bod yn rhaid i'r ymgeisydd:

- feddu ar broses ar gyfer creu a chymeradwyo cyfrifon defnyddwyr
- dilysu defnyddwyr cyn rhoi mynediad at gymwysiadau neu ddyfeisiau, gan ddefnyddio manylion unigryw (gweler dilysu seiliedig ar gyfrinair)
- dileu neu analluogi cyfrifon defnyddwyr pan nad oes eu hangen mwyach (pan fydd defnyddiwr yn gadael y sefydliad neu ar ôl cyfnod penodol pan nad yw'r cyfrif yn weithredol, er enghraifft)
- rhoi dull dilysu aml-ffactor ar waith, pan fydd ar gael. Rhaid defnyddio dull dilysu aml-ffactor bob amser ar gyfer gwasanaethau cwmwl.
- defnyddio cyfrifon ar wahân i gyflawni gweithgareddau gweinyddol yn unig (dim anfon negeseuon e-bost, pori'r we nac ymgymryd â gweithgareddau defnyddiwr safonol eraill a all amlygu breintiau gweinyddol i risgiau y gellir eu hosgoi)

- dileu neu analluogi breintiau mynediad arbennig pan na fydd eu hangen mwyach (pan fydd aelod o'r staff yn newid rôl, er enghraifft)

Dilysu seiliedig ar gyfrinair

Mae angen i'r defnyddiwr ymgymryd â dull dilysu ar gyfer pob cyfrif defnyddiwr.

Lle y defnyddir cyfrinair i wneud hyn, dylid defnyddio'r mesurau diogelwch canlynol:

- Caiff cyfrineiriau eu diogelu rhag ymosodiad nerth bôn braich sy'n gysylltiedig â dyfalu cyfrineiriau drwy roi o leiaf un o'r canlynol ar waith:
    - defnyddio dull dilysu aml-ffactor (gweler isod)
    - arafu nifer yr ymgeisiau *(throttling)*. Mae hyn yn golygu bod yr amser y mae'n rhaid i ddefnyddiwr aros rhwng pob ymgais yn cynyddu gyda phob ymgais aflwyddiannus. Dylai hyn ganiatáu 10 o gynigion ar y mwyaf mewn 5 munud.
    - cloi cyfrifon ar ôl 10 ymgais aflwyddiannus ar y mwyaf

- Defnyddir rheolaethau technegol i reoli ansawdd cyfrineiriau. Bydd hyn yn cynnwys un o'r canlynol:
    - defnyddio dull dilysu aml-ffactor (gweler isod)
    - cyfrinair sy'n cynnwys o leiaf 12 o nodau, heb unrhyw gyfyngiadau ar uchafswm y nodau
    - cyfrinair sy'n cynnwys o leiaf 8 nod, heb unrhyw gyfyngiadau ar uchafswm y nodau, a rhwystro cyfrineiriau cyffredin yn awtomatig gan ddefnyddio rhestr gwrthod.

- Caiff pobl eu helpu i ddewis cyfrineiriau unigryw ar gyfer eu cyfrifon gwaith. Gwneir hyn drwy:
    - addysgu pobl sut i osgoi cyfrineiriau cyffredin neu gyfrineiriau darganfyddadwy, fel enw anifail anwes, patrymau bysellfwrdd cyffredin neu gyfrineiriau y maent wedi'u defnyddio mewn mannau eraill. Gallai hyn gynnwys addysgu pobl sut i ddefnyddio'r nodwedd cynhyrchu cyfrinair sy'n rhan o rai adnoddau rheoli cyfrineiriau.
    - annog pobl i ddewis cyfrineiriau hwy. Gellir gwneud hyn drwy hyrwyddo'r defnydd o sawl gair gwahanol (o leiaf dri) i greu cyfrinair, (e.e., 'Tri Gair Ar Hap')

    - darparu lle storio diogel ar gyfer cyfrineiriau (er enghraifft adnodd rheoli cyfrineiriau neu gabinet diogel wedi'i gloi) gyda gwybodaeth glir am sut a phryd y gellir ei ddefnyddio.
    - peidio â gorfodi dyddiad dod i ben rheolaidd ar gyfer cyfrineiriau
    - peidio â gorfodi gofynion cymhlethdod ar gyfer cyfrineiriau

- Mae yna broses sefydledig ar gyfer newid cyfrineiriau yn brydlon os bydd yr ymgeisydd yn gwybod bod y cyfrinair neu'r cyfrif wedi'i beryglu neu os yw'n amau hynny.

Dilysu Aml-ffactor (MFA)

Yn ogystal â chynnig diogelwch ychwanegol ar gyfer cyfrineiriau na chânt eu diogelu gan reolaethau technegol eraill (uchod), dylid defnyddio dull dilysu aml-ffactor bob amser i sicrhau bod cyfrifon gweinyddol, a chyfrifon y gellir cael gafael arnynt o'r rhyngrwyd, yn fwy diogel.

Mae'n rhaid i gyfrinair sy'n gysylltiedig â dull dilysu aml-ffactor gynnwys o leiaf 8 nod, heb unrhyw gyfyngiadau ar uchafswm y nodau.

Mae pedwar math o ffactor ychwanegol y gellir eu hystyried:

- dyfais a reolir/dyfais menter
- ap ar ddyfais ddibynadwy
- tocyn a gedwir ar wahân
- cyfrif hysbys neu ddibynadwy

Dylid dewis ffactorau ychwanegol sy'n ddefnyddadwy ac yn hygyrch. Efallai y bydd angen cynnal profion i gadarnhau a yw ffactor yn addas ar gyfer y defnyddwyr. I gael rhagor o wybodaeth, gweler canllawiau NCSC ar Dilysu Aml-ffactor.

> **Gwybodaeth** Mae yna ddulliau dilysu aml-ffactor sy'n fwy diogel na SMS, ond mae'n dal i gynnig mantais enfawr o gymharu â pheidio â defnyddio unrhyw ddull dilysu aml-ffactor. Mae unrhyw ddull dilysu aml-ffactor yn well na dim un o gwbl. Fodd bynnag, os oes dewisiadau amgen ar gael a fydd yn addas ar eich cyfer, argymhellwn eich bod yn defnyddio'r rhain yn hytrach na SMS.

Diogelwch rhag maleiswedd

Yn gymwys i'r canlynol: Gweinyddion, cyfrifiaduron bwrdd gwaith, gliniaduron, llechi, ffonau symudol, IaaS, PaaS, SaaS.

Amcan

Cyfyngu ar weithredu maleiswedd hysbys a meddalwedd annibynadwy er mwyn atal codau niweidiol rhag achosi difrod neu gyrchu data sensitif.

Cyflwyniad

Gall gweithredu meddalwedd a gaiff ei lawrlwytho o'r rhyngrwyd amlygu dyfais i haint maleiswedd. Mae maleiswedd, megis feirysau, mwydod ac ysbïwedd cyfrifiadurol, yn feddalwedd sydd wedi'i hysgrifennu a'i dosbarthu'n fwriadol i gyflawni gweithredoedd maleisus. Gall ffynonellau heintiau maleiswedd gynnwys: atodiadau e-bost maleisus, lawrlwythiadau (gan gynnwys y rhai o storfeydd cymwysiadau) a gosod meddalwedd anawdurdodedig yn uniongyrchol.

Os caiff system ei heintio â maleiswedd, bydd eich sefydliad yn debygol o wynebu problemau fel systemau nad ydynt yn gweithio'n iawn, colli data, neu haint a drosglwyddir i fannau eraill na wyddys amdano nes y bydd yn achosi difrod rhywle arall.

Gallwch osgoi'r difrod posibl a wneir gan faleiswedd i raddau helaeth drwy wneud y canlynol:

- canfod ac analluogi maleiswedd cyn y gall achosi difrod (meddalwedd wrthfaleiswedd)
- gweithredu meddalwedd rydych yn gwybod y gallwch ddibynnu arni (rhestr caniatáu)
- gweithredu meddalwedd annibynadwy mewn amgylchedd sy'n rheoli mynediad at ddata eraill (*sandboxing*)

Enghraifft

> Mae Corfforaeth Acme yn defnyddio dull llofnodi codau ochr yn ochr â rheol sydd ond yn caniatáu gweithredu cymwysiadau sydd wedi'u fetio o storfa gymwysiadau'r ddyfais ar ddyfeisiau. Ni fydd cymwysiadau heb eu llofnodi a chymwysiadau anghymeradwy yn rhedeg ar ddyfeisiau. Mae'r ffaith mai dim ond cymwysiadau dibynadwy (rhai ar restr o gymwysiadau a ganiateir) y gall defnyddwyr eu gosod yn arwain at lai o risg y bydd haint maleiswedd.

Gofynion o dan y thema rheolaeth dechnegol hon

Rhaid i'r ymgeisydd roi dull diogelu rhag maleiswedd ar waith ar bob dyfais sydd o fewn y cwmpas. Ar gyfer pob dyfais i'r fath, rhaid i'r ymgeisydd ddefnyddio o leiaf un o'r tri dull a restrir isod:

Meddalwedd wrthfaleiswedd

- Rhaid sicrhau bod y feddalwedd (a phob ffeil llofnod maleiswedd gysylltiedig) yn gyfredol, a bod ffeiliau llofnod yn cael eu diweddaru o leiaf bob dydd. Gellir gwneud hyn drwy ddiweddariadau awtomataidd, neu adnodd a reolir yn ganolog.
- Rhaid i'r feddalwedd gael ei ffurfweddu i sganio ffeiliau yn awtomatig pan geir mynediad atynt. Mae hyn yn cynnwys pan gaiff ffeiliau eu lawrlwytho a'u hagor, a phan geir mynediad atynt o ffolder rhwydwaith.
- Rhaid i'r feddalwedd sganio tudalennau gwe yn awtomatig pan geir mynediad atynt drwy borwr gwe (boed hynny drwy feddalwedd arall neu drwy'r porwr ei hun).
- Rhaid i'r feddalwedd atal cysylltiadau â gwefannau maleisus ar y rhyngrwyd (drwy restr gwrthod, er enghraifft) – oni bai bod angen busnes clir wedi'i ddogfennu a bod yr ymgeisydd yn deall ac yn derbyn y risg gysylltiedig.

Rhestr caniatáu cymwysiadau

- Dim ond cymwysiadau cymeradwy, a gyfyngir gan ddull llofnodi codau, y caniateir iddynt weithredu ar ddyfeisiau. Rhaid i'r ymgeisydd wneud y canlynol:
    - cymeradwyo'r cyfryw gymwysiadau cyn eu gosod ar ddyfeisiau
    - cynnal rhestr gyfredol o gymwysiadau cymeradwy. Ni ddylai defnyddwyr allu gosod unrhyw gymhwysiad heb ei lofnodi neu gymhwysiad sydd â llofnod annilys.

Profi cymwysiadau (*sandboxing)*

- Rhaid i unrhyw god nad yw ei darddiad yn hysbys gael ei redeg o fewn amgylchedd profi (*sandbox*) sy'n atal mynediad at adnoddau eraill oni fydd y defnyddiwr yn rhoi caniatâd penodol. Mae hyn yn cynnwys y canlynol:
    - cymwysiadau eraill mewn amgylchedd profi (*sandboxed*)
    - storfeydd data, megis y rhai sy'n storio dogfennau a ffotograffau
    - perifferolion sensitif, megis camera, microffon a GPS
    - mynediad rhwydwaith lleol

Rheoli diweddariadau diogelwch

Yn gymwys i'r canlynol: gweinyddion, cyfrifiaduron bwrdd gwaith, gliniaduron, llechi, ffonau symudol, waliau tân, llwybryddion, IaaS, PaaS, SaaS.

Amcan

Sicrhau nad yw dyfeisiau a meddalwedd yn agored i broblemau diogelwch hysbys y gellir eu datrys.

Cyflwyniad

Gall unrhyw ddyfais sy'n rhedeg meddalwedd gynnwys ddiffygion diogelwch, a elwir yn ‘wendidau’.

Caiff gwendidau eu darganfod yn rheolaidd mewn pob math o feddalwedd. Unwaith y cânt eu darganfod, bydd unigolion neu grwpiau maleisus yn symud yn gyflym i gamddefnyddio (neu ‘fanteisio ar’) wendidau er mwyn ymosod ar gyfrifiaduron a rhwydweithiau mewn sefydliadau â'r gwendidau hyn.

Rhybudd

> Mae'r rheini sy'n gwerthu cynnyrch yn cynnig atebion ar gyfer gwendidau a nodir yn y cynhyrchion a gefnogir ganddynt o hyd ar ffurf diweddariadau meddalwedd a elwir yn ‘batsys’ neu ddiweddariadau diogelwch. Gall y rhain fod ar gael i gwsmeriaid ar unwaith neu gallant gael eu rhyddhau'n rheolaidd (efallai'n fisol).

Gofynion o dan y thema rheolaeth dechnegol hon

Rhaid i'r ymgeisydd sicrhau bod yr holl feddalwedd o fewn y cwmpas yn gyfredol. Rhaid i'r holl feddalwedd ar ddyfeisiau o fewn y cwmpas:

- fod yn drwyddedig ac wedi'i chefnogi
- cael ei dileu o ddyfeisiau pan na chaiff ei chefnogi mwyach neu ei dileu o'r cwmpas drwy ddefnyddio “is-set” ddiffiniedig sy'n atal pob traffig i fynd i'r rhyngrwyd ac oddi yno
- cynnwys diweddariadau awtomatig a alluogir lle y bo'n bosibl
- cael eu diweddaru, gan gynnwys cymhwyso unrhyw newidiadau ffurfweddu y mae angen eu gwneud â llaw er mwyn sicrhau bod y diweddariad yn effeithiol, o fewn 14 diwrnod* i ryddhau diweddariad, lle:
    - Bydd y diweddariad yn mynd i'r afael â gwendidau a ddisgrifir gan y gwerthwr fel rhai ‘critigol’ neu ‘risg uchel’
    - Bydd y diweddariad yn mynd i'r afael â gwendidau â sgôr CVSS v3 o 7 neu uwch

- Nid yw'r gwerthwr yn rhoi unrhyw fanylion ynghylch lefel y gwendidau y bydd diweddariad yn mynd i'r afael â nhw

Er mwyn sicrhau'r diogelwch gorau posibl a phroses weithredu hawdd, argymhellir yn gryf bod **pob** diweddariad a ryddheir yn cael ei gymhwyso o fewn 14 diwrnod (ond nid yw'n orfodol).

*Mae'n bwysig bod y diweddariadau hyn yn cael eu cymhwyso cyn gynted â phosibl. Mae 14 diwrnod yn cael ei ystyried yn gyfnod rhesymol i allu bodloni'r gofyniad hwn. Byddai gadael hyn am gyfnod hwy yn peri risg ddifrifol o ran diogelwch ac efallai na fyddai'n ymarferol gwneud hynny yn gynt.

Gwybodaeth

> Os yw'r gwerthwr yn defnyddio termau gwahanol i ddisgrifio difrifoldeb gwendidau, gweler y diffiniad cywir yn y System Sgorio Gwendidau Cyffredin (CVSS). At ddibenion cynllun Cyber Essentials, gwendidau ‘critigol’ neu ‘risg uchel’ yw'r rhai sydd â sgôr CVSS3 o 7 neu uwch neu a gaiff eu nodi gan y gwerthwr fel rhai “critigol neu risg uchel”.

Rhybudd

> Bydd rhai gwerthwyr yn rhyddhau diweddariadau diogelwch ar gyfer amrywiaeth o faterion â lefelau gwahanol o ddifrifoldeb fel un diweddariad. Os bydd y cyfryw ddiweddariad yn cwmpasu unrhyw faterion ‘critigol’ neu ‘risg uchel’, yna rhaid iddo gael ei osod o fewn 14 diwrnod.

Canllawiau Pellach

Gwneud copi wrth gefn o'ch data

Mae'r broses hon yn golygu creu copi o'ch gwybodaeth a'i gadw ar ddyfais arall neu storfa cwmwl (ar-lein).

Drwy wneud copi wrth gefn o'ch data yn rheolaidd, bydd gennych fersiwn ddiweddar o'r wybodaeth a gadwyd gennych bob amser. Bydd hyn yn eich helpu i adfer yn gyflymach os caiff eich data eu colli neu eu dwyn.

Gallwch hefyd droi'r adnodd gwneud copi wrth gefn yn awtomatig ymlaen. Bydd yr adnodd hwn yn cadw eich gwybodaeth yn rheolaidd mewn storfa cwmwl, heb i chi orfod cofio gwneud hynny.

Os ydych yn cadw eich gwybodaeth ar gof bach USB neu yriant caled allanol, datgysylltwch ef o'ch cyfrifiadur pan nad ydych yn gwneud copi o'ch gwybodaeth.

Nid yw gwneud copi wrth gefn o'ch data yn un o ofynion technegol Cyber Essentials; fodd bynnag, rydym yn argymell yn gryf eich bod yn rhoi datrysiad priodol ar waith ar gyfer gwneud hynny.