National Cyber Security Centre
a part of GCHQ

CIOB

Seiberddiogelwch i fusnesau adeiladu

Canllawiau seiberddiogelwch ar gyfer busnesau bach a chanolig sy'n gweithio yn y diwydiant adeiladu a'r gadwyn gyflenwi ehangach

Rhagair

Sarah Lyons
Dirprwy Gyfarwyddwr Gwydnwch yr Economi a Chymdeithas yr NCSC

Mae'n bleser gan y Ganolfan Seiberddiogelwch Genedlaethol (NCSC) bartneru â'r Sefydliad Adeiladu Siartredig (CIOB) i gynhyrchu'r canllaw hwn i helpu busnesau adeiladu bach a chanolig i amddiffyn eu hunain rhag ymosodiadau seiber.

Yr NCSC yw arweinydd llywodraeth y Deyrnas Unedig ar gyfer seiberddiogelwch. Ein nod yw gwneud y Deyrnas Unedig y lle mwyaf diogel i fyw a gweithio ar-lein, ac i'n helpu i gyflawni hyn, rydym yn gweithio'n agos gyda sefydliadau allweddol o bob maint ar draws pob sector, gan gynnwys adeiladu.

Fel llawer o sectorau eraill sy'n cofleidio technolegau newydd ac yn mabwysiadu ffyrdd digidol newydd o weithio, mae'r diwydiant adeiladu yn parhau i gael ei effeithio gan droseddu seiber. Mae'r ddogfen hon yn cynnwys canllawiau seiberddiogelwch clir a chryno a all eich helpu i ddiogelu eich busnes.

Er na allwn warantu amddiffyniad yn erbyn yr holl fygythiadau seiber rydych chi'n eu hwynebu, trwy weithredu'r camau a ddisgrifir, byddwch yn cael eich amddiffyn rhag yr ymosodiadau seiber mwyaf cyffredin. A phe bai'r gwaethaf yn digwydd, dylech allu adfer yn gyflym.

Rydym bob amser yn ceisio gwella ein canllawiau, felly os oes gennych unrhyw adborth, da neu ddrwg, cysylltwch â ni gan ddefnyddio gwefan yr NCSC.

Caroline Gumble
Prif Weithredwr y Sefydliad Adeiladu Siartredig (CIOB)

Mae deall rôl seiberddiogelwch yn y diwydiant adeiladu bellach yn ofyniad hanfodol ar gyfer sefydliadau o bob maint. Mae asedau digidol yn gyffredin yn y rhan fwyaf o fusnesau (gan gynnwys y rheini yn y sector adeiladu), felly mae rheoli data a sianeli cyfathrebu digidol yn bwysicach nag erioed.

Ni ddylid diystyru canlyniadau seiberddiogelwch diffygiol. Gall gael effaith ddinistriol ar elw ariannol, y rhaglen adeiladu, enw da busnes, perthnasoedd cadwyn gyflenwi, yr ased adeiledig ei hun ac, yn waethaf oll, iechyd a lles pobl. Felly mae deall agweddau digidol busnes (ac yna lleihau a rheoli'r risgiau a gyflwynir) yn hollbwysig.

Mae seiberddiogelwch wedi cael ei amlygu gan y CIOB ers peth amser. Mae ein Grŵp Diddordeb Arbennig Technolegau Digidol a Rheoli Asedau wedi cefnogi aelodau a'r diwydiant ehangach (gan gyfeirio'n benodol at gadwyni cyflenwi a chysylltiadau â chleientiaid) i ddeall egwyddorion cynllunio diogelwch da, ac i annog y defnydd o fesurau dylunio i liniaru a rheoli'r risgiau posibl ar gyfer prosiectau adeiladu. Mae'n bleser gennym bellach ffurfio partneriaeth â'r Ganolfan Seiberddiogelwch Genedlaethol (NCSC) a'r Ganolfan Diogelu'r Seilwaith Cenedlaethol (CPNI) i gynhyrchu adnodd amhrisiadwy arall, y canllaw Seiberddiogelwch i fusnesau adeiladu.

Mae'r canllaw hwn yn gyfle amserol i ganolbwyntio ar y risgiau a gyflwynir gan seiberdroseddu. Mae wedi'i anelu'n benodol at y busnesau bach a chanolig sy'n ffurfio'r mwyafrif o gwmnïau adeiladu yn y Deyrnas Unedig, ac mae'n adnodd hygyrch a all helpu sefydliadau i ddeall ac atal troseddau seiber ar draws y sector.

Caroline Gumble

Ynglŷn â'r canllaw hwn

Mae'r canllaw hwn wedi'i anelu at fusnesau bach a chanolig sy'n gweithio yn y diwydiant adeiladu a'r gadwyn gyflenwi ehangach (gan gynnwys gweithgynhyrchu cyflenwadau adeiladu, tirfesur, a gwerthu adeiladau).

- **Anelir Adran 1** y canllaw hwn at berchnogion neu reolwyr busnes. Mae'r adran hon yn disgrifio pam mae seiberddiogelwch yn bwysig i'r diwydiant adeiladu, ac yna'n crynhoi'r bygythiadau seiber sy'n gysylltiedig â phob cam o'r broses adeiladu (dylunio, adeiladu a throsglwyddo).
- **Mae Adran 2** yn darparu canllawiau y gellir eu rhoi ar waith i wneud eich busnes adeiladu yn fwy gwydn yn erbyn ymosodiadau seiber cyffredin. Mae'r canllaw wedi'i anelu at staff sy'n gyfrifol am offer a gwasanaethau TG o fewn busnes adeiladu. Efallai y bydd busnesau llai heb unrhyw rôl o'r fath am ddechrau trwy ddarllen Canllaw Busnesau Bach yr NCSC.

Yn y canllaw hwn

Adran 1
Ar gyfer perchnogion a rheolwyr busnes

Pam mae seiberddiogelwch yn bwysig

Pwy sydd y tu ôl i ymosodiadau seiber?

Cam dylunio
Cam adeiladu
Cam trosglwyddo

Adran 2
Ar gyfer staff sy'n gyfrifol am TG

Canllawiau seiberddiogelwch

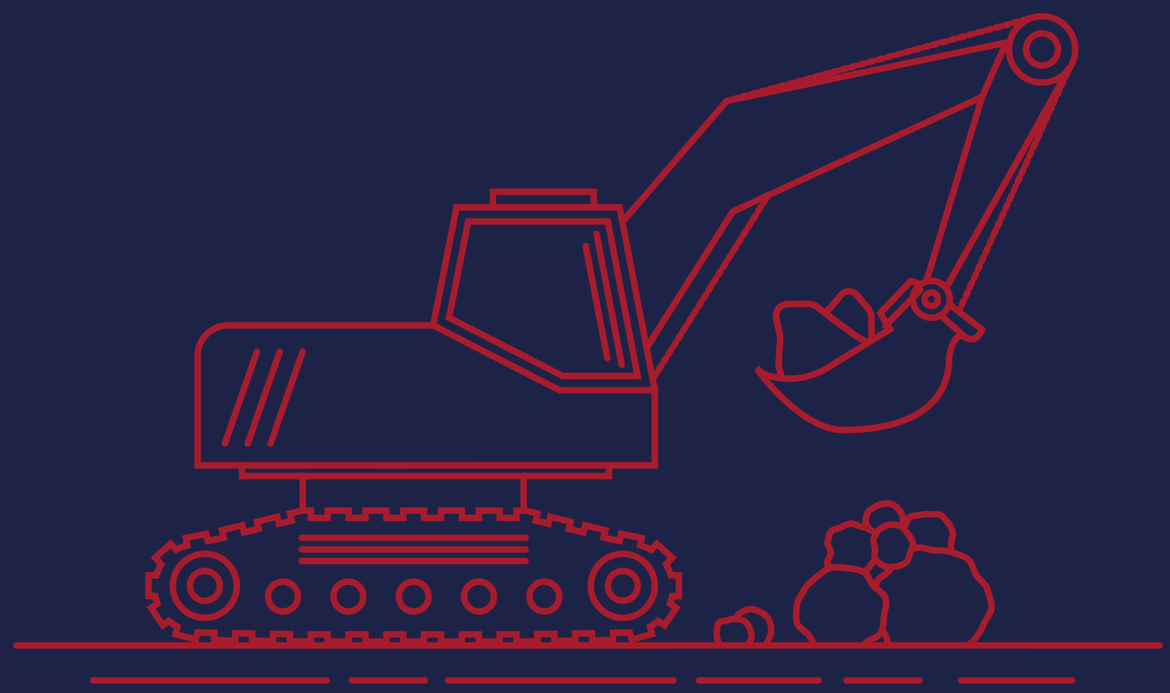
1. Gwneud copi wrth gefn o'ch data
2. Diogelu eich offer swyddfa rhag drwgwedd
3. Cadw'ch ffonau a'ch tabledi'n ddiogel
4. Defnyddio cyfrineiriau i ddiogelu'ch data
5. Delio â gwe-rwydo
6. Cydweithio â chyflenwyr a phartneriaid
7. Paratoi ar gyfer (ac ymateb i) ddigwyddiadau seiber

Ble i fynd am ragor o gymorth

Adran 1

Pam mae seiberddiogelwch yn bwysig

Ar gyfer perchnogion a rheolwyr busnes



Pam mae seiberddiogelwch yn bwysig

Mae ymosodiadau seiber proffil uchel diweddar yn erbyn y diwydiant adeiladu yn dangos sut mae busnesau o bob maint yn cael eu targedu gan droseddwyr.
Wrth i'r diwydiant barhau i gofleidio a mabwysiadu ffyrdd digidol newydd o weithio, mae'n bwysicach nag erioed deall sut y gallech fod yn agored i ymosodiadau seiber, a beth allwch chi ei wneud i amddiffyn eich busnes.

Mae seiberddiogelwch yn ymwneud â diogelu'r dechnoleg rydym yn dibynnu arni, a diogelu'r gwasanaethau a'r wybodaeth y mae ar bob busnes, mawr a bach, eu hangen i weithredu. Mae angen i'r diwydiant adeiladu gymryd y bygythiad seiber o ddifrif yn benodol am y rhesymau a ganlyn:

- Mae troseddwyr seiber yn gweld busnesau adeiladu fel targed hawdd, gyda llawer ohonynt â llifoedd arian uchel. Efallai'n ddealladwy, mae gan fusnesau llai a chanolig eu maint agwedd 'Dim ond busnes bach ydyn ni, ni fydd yn digwydd i ni' tuag at seiberddiogelwch, ac maent yn gyndyn o fuddsoddi amser, arian a hyfforddiant yn yr hyn y maent yn ei weld fel bygythiad annhebygol.
- Mae'r defnydd helaeth o isgontractwyr a chyflenwyr sy'n cynnwys nifer fawr o daliadau gwerth uchel yn gwneud busnesau adeiladu yn darged deniadol ar gyfer gwe-drywanu, sef pan fydd ymosodwyr yn anfon e-bost targedig sy'n esgus ei fod gan sefydliad cyfreithlon, mewn ymgais i dwyllo'r busnes adeiladu i dalu arian i mewn i gyfrif troseddwr.
- Er nad yw busnesau adeiladu yn storio'r un math o wybodaeth ariannol ag y mae banc, maent yn dal i storio (a chael mynediad at) ddata gwerthfawr. Gallai troseddwyr fod yn chwilio am fanylion am gais nesaf y cwmni (neu ddyluniad adeilad) er mwyn cael mantais annheg. Efallai bod seiberdroseddwyr yn chwilio am ddata sensitif gweithwyr, fel rhifau nawdd cenedlaethol, rhifau cyfrif banc a data cyflogres, er mwyn cyflawni lladrad hunaniaeth, neu greu e-byst realistig eu golwg ar gyfer ymosodiadau gwe-rwydo.

Efallai nad ydych yn sylweddoli, ond waeth beth fo maint a natur eich busnes, mae'r wybodaeth sydd gennych o werth i droseddwr. Ac er efallai na fyddant yn targedu eich busnes yn uniongyrchol, mae'n hawdd iawn cael eich niweidio gan e-byst gwe-rwydo y mae seiberdroseddwyr yn eu hanfon, yn ddiwahân, at filiynau o fusnesau.

Hyd yn oed os na fyddwch yn colli arian yn uniongyrchol, gallai toriad data (sef pan fydd gwybodaeth a ddelir gan sefydliad yn cael ei dwyn neu ei chyrchu heb ganiatâd) neu ymosodiad meddalwedd wystlo achosi i'ch busnes gau i lawr dros dro tra bod y toriad yn cael ei ymchwilio, a systemau'n cael eu hadennill, yn ogystal â niwed i enw da cwsmeriaid a phartneriaid. Gallai hefyd eich gadael yn agored i ymchwiliad (a dirwyon) gan Swyddfa'r Comisiynydd Gwybodaeth (ICO).

Pwy sydd y tu ôl i ymosodiadau seiber?

Mae'r diwydiant adeiladu'n wynebu nifer o grwpiau ac unigolion sy'n ceisio manteisio a gwneud niwed, a dyna pam ei bod mor bwysig sicrhau pob agwedd ddigidol ar eich busnes. Efallai y cewch eich targedu gan:

Droseddwyr ar-lein: maent yn dda am nodi a chynnal ymosodiadau seiber i wneud arian, er enghraifft dwyn a gwerthu data sensitif, neu ddal systemau a gwybodaeth ar wystl.

Hacwyr ymgyrchu: unigolion â graddau amrywiol o arbenigedd, yn aml yn gweithredu mewn ffordd heb ei thargedu (efallai i brofi eu sgiliau eu hunain neu achosi aflonyddwch dim ond er mwyn gwneud). Gallai hyn gynnwys ymgyrchwyr gwleidyddol, yn awyddus i brofi pwynt am resymau gwleidyddol neu ideolegol ac amgylcheddol, neu i amlygu neu ddifrïo gweithgareddau eich busnes.

Unigolion maleisus yn y busnes: maent yn defnyddio eu mynediad at ddata neu rwydweithiau busnes i gynnal gweithgaredd maleisus, megis dwyn gwybodaeth sensitif i'w rhannu â chystadleuwyr.

Gwladwriaethau cenedlaethol: yn targedu sefydliadau yn y sector cyhoeddus a phreifat. Hyd yn oed os nad ydych yn meddwl eich bod yn ddigon mawr i fod o ddiddordeb i lywodraethau tramor, dylech ddeall y gwerth y gallech ei gynrychioli. Efallai eich bod yn gweithio gyda sefydliadau mwy (neu ar brosiectau'r llywodraeth) sef eu prif darged.

Pam mae seiberddiogelwch yn bwysig

Mae'r tri cham allweddol yn y diwydiant adeiladu (dylunio, adeiladu a throsglwyddo) i gyd yn cynnwys llifoedd gwaith digidol helaeth, felly mae pob un ohonynt mewn perygl.

Popeth o'r cyfrifiaduron, ffonau a thabledi a ddefnyddir i gyrchu e-byst, i'r feddalwedd hanfodol a ddefnyddir i brosesu a storio gwybodaeth, i offer safle soffistigedig a systemau digidol sydd wedi'u gosod mewn adeiladau. Ac wrth gwrs, trwy gydol y broses adeiladu gyfan, bydd angen i chi reoli a diogelu gwybodaeth eich busnes (gan gynnwys gwybodaeth cleientiaid, staff a phrosiect).

Bydd camau cynnar y broses adeiladu, megis y broses dendro, yn cynhyrchu er enghraifft, dyfynbrisiau manwl a chontractau wedi'u llofnodi. Gallai ymosodiad seiber ar y cam hwn atal busnes rhag gallu ennill tendrau cyfredol am waith, ac effeithio ar gyfleoedd yn y dyfodol. Drwy roi'r canllawiau yn y ddogfen hon ar waith, bydd eich busnes mewn sefyllfa fwy diogel a gwydn yn erbyn ymosodiadau seiber. Byddwch hefyd yn ei chael hi'n haws cael ardystiadau cysylltiedig (fel Hanfodion Seiber ac ISO27001) a all ddangos rhywfaint o aeddfedrwydd seiber y mae rhai contractau'r llywodraeth ei angen.

Cam dylunio

Cam adeiladu

Cam trosglwyddo

Gofalu am ddogfennau a data hanfodol

Mae'n bwysig bod gennych system yn ei lle i dderbyn, olrhain a storio dogfennau electronig a phapur. Dylai'r system, boed yn ffisegol neu'n ddigidol (neu gyfuniad o'r ddau) reoli mynediad at wybodaeth sensitif, yn ogystal â chynnal 'edefyn aur' o wybodaeth (cofnodion gwybodaeth o ansawdd a chyfredol trwy gydol cylch oes yr ased) sy'n hanfodol i brosiect neu drafodion busnes. Argymhellwyd hyn yn flaenorol yn yr Adolygiad Annibynnol o Reoliadau Adeiladu a Diogelwch Tân: adolygiad Hackitt.

Mae cael system ar waith i gadw cofnodion o **beth** sydd wedi'i rannu, **pryd**, a chyda **phwy** yn helpu atal y bobl anghywir rhag cael mynediad at wybodaeth sensitif, megis manylion cleient neu weithiwr. Dylech hefyd gymryd camau i ddiogelu eich busnes fel bod staff, cyflenwyr, contractwyr a thrydydd partïon eraill ond yn cael mynediad at yr adnoddau sydd eu hangen i wneud eu gwaith. Mae'r awdurdodiad hwn yn helpu rheoli pwy sydd â mynediad at eich asedau ffisegol a digidol, ac mae'n cael sylw manwl yng nghanllawiau'r NCSC ar Hunaniaeth a rheoli mynediad.

Ymgysylltu a hyfforddiant

Ar bob cam o waith adeiladu, mae'n bwysig sicrhau eich bod yn cyfathrebu gofynion seiberddiogelwch gyda'ch staff, ar y safle ac mewn unrhyw leoliadau anghysbell. **Mae pwysigrwydd - er enghraifft - gwisgo het galed, yn hunanesboniadol. I'r gwrthwyneb, gallai esbonio'r perygl o glicio ar ddolenni o fewn e-byst amheus fod yn anoddach eu gwerthu, yn enwedig o fewn busnes adeiladu lle mae'r swyddogaeth TG yn llai amlwg.**

Mae seiberddiogelwch da yn ystyried sut mae pobl yn gweithio'n ymarferol, ac nid yw'n creu baich arnynt o ran prosesau neu weithdrefnau sy'n eu rhwystro rhag cyflawni eu swyddi. Mae cefnogi eich staff i ennill y sgiliau a'r wybodaeth sydd eu hangen i weithio'n ddiogel yn aml yn cael ei wneud trwy gyfrwng ymwybyddiaeth neu hyfforddiant. Os ydych yn cynnal sesiynau briffio diogelwch ar gyfer ymwelwyr neu staff, defnyddiwch nhw i roi arweiniad (gan gynnwys ar seiberddiogelwch) ac i godi ymwybyddiaeth o ddiogelwch.

Yn gyffredinol mae staff eisiau gwneud y peth iawn, ond gall diffyg dealltwriaeth ynghylch pam y gofynnir iddynt wneud (neu beidio â gwneud) rhywbeth ymddangos fel 'diogelwch er ei fwyn ei hun'. Ceisiwch addysgu staff ar ddiogelwch mewn ffordd gadarnhaol, yn hytrach na defnyddio dychryn. Canolbwyntiwch ar sut mae eu gweithredoedd yn cael effaith gadarnhaol, yn hytrach na'r drafferth y byddant ynddi os byddant yn gwneud camgymeriad.

Er mwyn addysgu gweithwyr ar seiberddiogelwch, mae'r NCSC wedi datblygu pecyn e-ddysgu 'Awgrymiadau Da i Staff', y gellir ei gwblhau ar-lein.

Pam mae seiberddiogelwch yn bwysig

Cam dylunio

Y cam dylunio yw'r broses o ddatblygu briff y prosiect fel y gellir adeiladu'r adeilad. Mae llawer o'r cam hwn yn cael ei wneud yn ddigidol, ac mae'n debygol eich bod yn defnyddio amrywiaeth eang o wahanol offer meddalwedd yn ystod y broses ddylunio, megis:

- dylunio trwy gymorth cyfrifiadur (CAD) a phecynnau modelu 3D
- offer cydweithio ar gyfer rhannu gwybodaeth prosiect
- pecynnau efelychu i gynorthwyo gyda'r disgyblaethau strwythurol a pheirianneg arbenigol eraill
- systemau TG cyffredinol ar gyfer storio gwybodaeth a data (naill ai'n lleol neu ar rwydwaith busnes

Mae'n bwysig iawn gwneud yn siŵr bod y feddalwedd yn cael ei diweddaru bob amser. Mae cymhwyso'r diweddariadau hyn (proses a elwir yn glytio) yn un o'r pethau pwysicaf y gallwch eu gwneud i wella seiberddiogelwch.

Ar rai prosiectau, gallwch ymuno neu greu Amgylchedd Data Cyffredin (CDE) gyda busnesau eraill. Mae'r amgylcheddau hyn yn cynnwys llawer iawn o wybodaeth am brosiectau gan ganiatáu mynediad i drydydd partïon. Gall canllaw hunaniaeth a rheoli mynediad yr NCSC eich helpu i reoli pwy all (a phwy na all) gael mynediad i'ch data. Dylech hefyd roi proses 'angen gwybod' ar waith, ble caniateir mynediad i wybodaeth sydd ei hangen ar gyfer y dasg honno yn unig, a sicrhau bod staff yn cael eu tynnu o'r rhestr pan fyddant yn gadael y prosiect neu fusnes.

Asesiad risg seiberddiogelwch

Mae asesiad risg yn rhan hanfodol o unrhyw brosiect adeiladu, a dylai hyn gynnwys risgiau seiberddiogelwch (yn ogystal â rhai iechyd a diogelwch hirsefydlog). Mae cynnal asesiad risg seiberddiogelwch ar ddechrau'r prosiect yn eich galluogi i nodi pa risgiau seiberddiogelwch y gallai eich busnes eu hwynebu, ac i gynnwys camau rhagofalus y gallwch eu cymryd.

Mae seiberddiogelwch yn ymwneud cymaint â gwybod sut mae eich busnes yn gweithredu ag ydyw â thechnoleg. Meddyliwch am ba bobl, gwybodaeth, technolegau a phrosesau busnes sy'n hanfodol i'ch busnes. Beth fyddai'n digwydd pe na bai gennych fynediad atynt mwyach (neu pe na bai gennych reolaeth drostynt mwyach)? Dylai'r ddealltwriaeth sylfaenol hon o **beth** sy'n bwysig i chi, a **pham** ei fod yn bwysig, eich helpu i flaenoriaethu ble i amddiffyn eich busnes fwyaf.

Yna dylid nodi gofynion seiberddiogelwch a'u gweithredu i reoli'r risgiau a aseswyd. Mae hyn yn cynnwys mynediad at wybodaeth, mynediad at systemau a meddalwedd TG a mynediad i swyddfeydd a safleoedd. Dylech barhau i ailymweld ac adnewyddu eich asesiad wrth i'r prosiect ddatblygu i sicrhau eich bod yn parhau i reoli risgiau'n effeithiol.

I gael rhagor o wybodaeth am ddefnyddio asesiadau risg i wella seiberddiogelwch, cyfeiriwch at ganllaw Pecyn Cymorth Bwrdd yr NCSC.

Pam mae seiberddiogelwch yn bwysig

Cam Adeiladu

O'i gymharu â'r cam dylunio, mae gweithgareddau yn ystod y cam adeiladu fel arfer yn gofyn am weithlu mwy, mwy o ddeunyddiau ac offer, a mwy o ryngweithio â thrydydd partïon. Wrth i gymhlethdod a maint prosiect gynyddu yn ystod y gwaith adeiladu, bydd busnesau'n canolbwyntio'n naturiol ar gyflawniadau a therfynau amser y prosiect. Mae'n bwysig nad yw diogelwch yn cael ei ddiystyru ar y cam hwn o'r prosiect.

Diogelu safleoedd adeiladu ac offer uwch-dechnoleg

Mae'r defnydd o offer uwch-dechnoleg i arolygu adeiladau neu safleoedd yn dod yn fwyfwy cyffredin. Gall dronau ac offer GPS greu modelau a delweddiadau manwl. Gallai'r data a'r wybodaeth a gesglir hefyd gynnwys asedau cyfagos, boed uwchlaw'r ddaear neu o dan y ddaear.

Gall offer fod yn darged i ladron, ar gyfer ailwerthu ac yn enwedig os ydynt yn storio data safle, prosiect neu ddata sensitif. Er efallai na fydd rhai offer yn arbennig o ddrud i'w hadnewyddu (er enghraifft camera neu ddyfais GPS), gallai'r data sy'n cael ei storio arnynt fod yn werthfawr iawn i ymosodwr seiber. Dylech ddiogelu offer arolygu, camerâu, cyfrifiaduron llechen, offer codi ac ati, i atal eu lladrad ac unrhyw ddata sy'n cael ei storio arnynt. Mae teledu cylch cyfyng a thechnolegau diogelwch eraill yn darparu amddiffyniad sylweddol yn erbyn lladrad achlysurol a manteisgar.

Ystyriwch sut mae offer TG a ddefnyddir ar safleoedd adeiladu yn wahanol i offer yn y swyddfa. Er enghraifft, efallai y bydd y safle ei hun yn llai diogel, neu efallai bod prinder lle/dim lle i gadw eich offer TG yn ddiogel. Mae'n bosibl y bydd mynediad cyfyngedig i rwydweithiau neu wasanaethau eich busnes. Efallai nad oes gennych chi unrhyw gysylltiad (neu gyfyngedig) â'r rhyngrwyd hyd yn oed. Gall yr holl ffactorau hyn ei gwneud hi'n anoddach cyrchu a diogelu eich data. Gall offer TG sy'n cael ei adael neu ei storio mewn cerbydau neu swyddfa safle fod yn arbennig o agored i ladron manteisgar.

Dylech hefyd ystyried pa ddata personol sy'n cael eu storio ar safle adeiladu. Er enghraifft, manylion unigolion a'u cysylltiadau argyfwng, data biometrig, ac adroddiadau digwyddiadau iechyd a diogelwch. Cofiwch fod y wybodaeth hon yn bersonol ac yn dod o dan ddeddfwriaeth diogelu data a dylid ei diogelu yn unol â hynny. Mae'r NCSC yn darparu gwybodaeth am GDPR a'r hyn y mae'n ei olygu i seiberddiogelwch.

Technoleg ddigidol a systemau cysylltiedig

Os ydych chi'n ymwneud mewn unrhyw ffordd â'r canlynol:

- systemau rheoli adeiladau (BMS)
- systemau awtomeiddio a rheoli adeiladau (BACS)
- systemau rheoli ynni adeiladau (BEMS)
- systemau awtomeiddio a rheoli diwydiannol (IACS)

- yna yn ogystal â'ch gofynion rheoleiddiol, bydd angen i chi ystyried yr agweddau seiberddiogelwch. Mae hyn y tu hwnt i gwmpas y ddogfen hon, felly cyfeiriwch at yr adnoddau canlynol:

- Cod Ymarfer IET 2021 ar gyfer Seiberddiogelwch yn yr Amgylchedd Adeiledig (a noddir gan yr NCSC)
- Egwyddorion Seiberddiogelwch Llefydd Cysylltiedig yr NCSC

Pam mae seiberddiogelwch yn bwysig

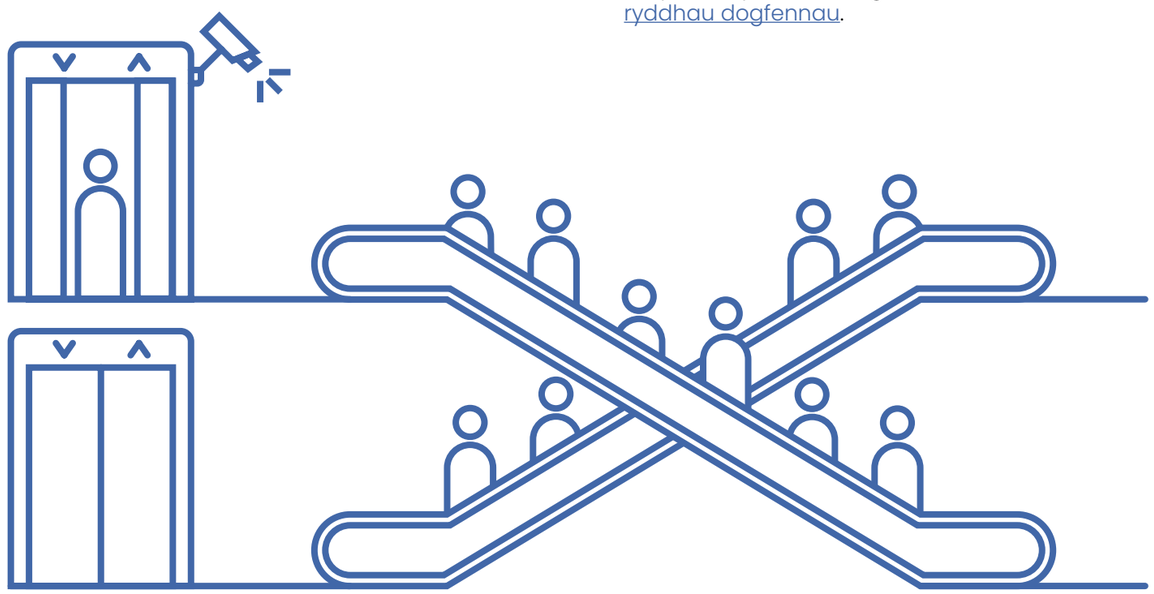
Cam Trosglwyddo

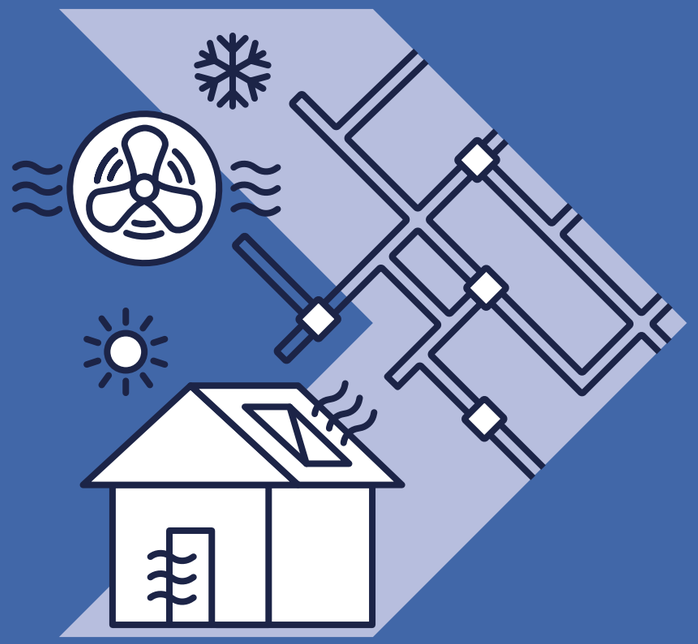
Ar ôl cwblhau'r prosiect, efallai y bydd systemau rheoli adeiladau wedi'u gosod (er enghraifft BMS, BACS, BEMS ac IACS). Mae'n bwysig bod y systemau hyn yn cael eu trosglwyddo i'r cleient fel y gallant barhau i ddiogelu'r adeilad ac unrhyw systemau digidol y gallai eu cynnwys.

Bydd y systemau a osodir yn dibynnu ar natur a defnydd y prosiect, ond gallant gynnwys cyfuniadau o'r canlynol:

- awtomeiddio a rheoli goleuadau
- gwresogi, awyru ac aerdymheru (HVAC)
- tân, canfod mwg a larymau
- synwyryddion symudiad, TCC, a rheoli mynediad
- lifftiau a grisiau symudol
- prosesau neu offer diwydiannol
- dyfeisiau cysgodi
- rheoli ynni a mesuryddion

Mae'n hynod bwysig bod y rhain yn cael eu dogfennu'n llawn, a bod holl fanylion gosod, gweithredu a chynnal a chadw yn cael eu cynnwys mewn unrhyw drosglwyddiad i'r cleient neu weithredwr yr adeilad. Dylai'r manylion hyn gynnwys unrhyw gamau a gymerwyd i ddiogelu'r systemau yn ogystal ag unrhyw gamau neu ddogfennaeth sydd eu hangen i gynnal diogelwch y systemau hyn drwy gydol eu hoes. Mae'n debygol y byddwch yn cadw gwybodaeth sy'n ymwneud â'r prosiect ar ôl ei drosglwyddo at ddibenion yswiriant. I gael gwybodaeth fanylach, cyfeiriwch at ganllawiau'r CPNI ar ryddhau dogfennau.

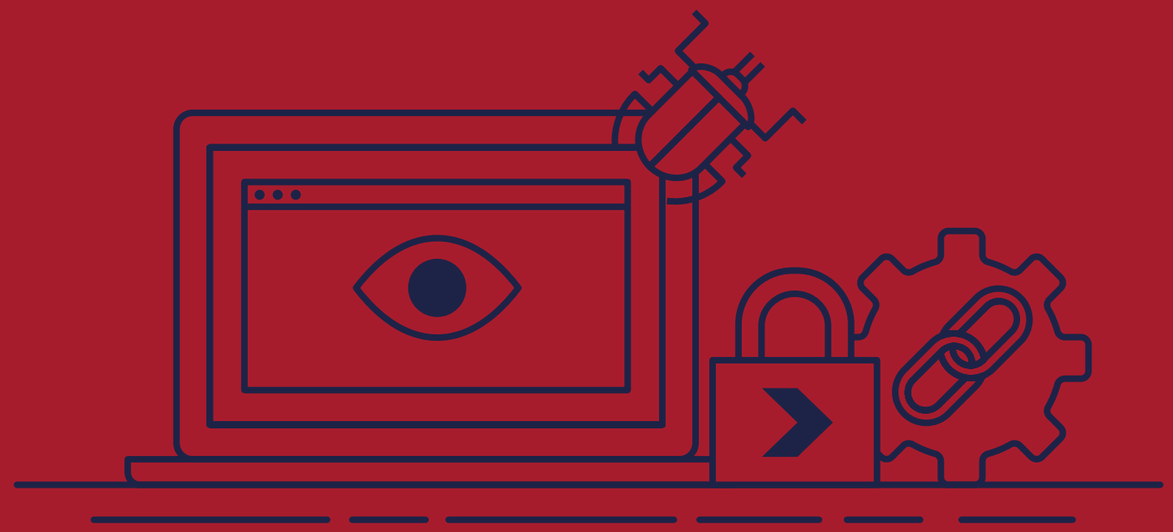




Adran 2

Cyngor a Chanllawiau

Ar gyfer staff sy'n gyfrifol am TG



Canllawiau seiberddiogelwch

Bydd dilyn y camau a ddisgrifir yn yr adran hon yn lleihau'r tebygolrwydd y bydd eich busnes adeiladu'n dioddef ymosodiad seiber, a bydd yn eich helpu i ddod yn ôl ar eich traed pe bai'r gwaethaf yn digwydd.

01
Creu copi wrth gefn o'ch data

Meddyliwch faint rydych chi'n dibynnu ar eich data busnes-gritigol, fel cynlluniau prosiect, modelau CAD, manylion cwsmeriaid, dyfynbrisiau, archebion, a manylion talu. Nawr dychmygwch pa mor hir y byddech chi'n gallu gweithredu hebddynt.

Mae'n bwysig cadw copi wrth gefn o'r wybodaeth hanfodol hon rhag ofn y bydd rhywbeth yn digwydd i'ch offer TG, neu safle eich busnes. Gallai fod damwain (fel tân, llifogydd, neu golled), gallech gael offer wedi'i ddwyn, neu fe allai meddalwedd wystlo (neu ddrwgwedd arall) niweidio, ddileu neu gloi eich data.

Nodwch yr hyn y mae angen i chi gadw wrth gefn

Dechreuwch drwy nodi'ch gwybodaeth bwysicaf (hynny yw, y wybodaeth na allai eich busnes weithredu hebddi neu y mae'n ofynnol yn gyfreithiol i chi ei diogelu). Gwnewch gopi wrth gefn ar gof bach USB, gyriant caled allanol, neu 'yn y cwmwl'. Ar ôl gwneud eich copi wrth gefn, gwnewch yn siŵr eich bod yn gwybod sut i adennill y wybodaeth ohono. I'ch rhoi ar ben ffordd, dyma rai canllawiau 'sut-i' ar gyfer sefydlu storfa cwmwl:

- Apple (iPhone, iPad ac iPod Touch, a Mac)
- Google (Android)
- Dyfeisiau Microsoft (Windows 10).

Cadwch eich copi wrth gefn ar wahân i'ch cyfrifiadur

P'un a yw ar gof bach USB, ar yriant ar wahân neu gyfrifiadur ar wahân, dylid cyfyngu ar fynediad at gopïau wrth gefn fel:

- bod dim ond staff priodol yn gallu cael mynediad
- nad ydynt wedi'u cysylltu'n barhaol (naill ai'n gorfforol neu dros gyfnod o amser dros gysylltiad rhwydwaith) i'r ddyfais sy'n dal y copi gwreiddiol

Mae defnyddio storfa cwmwl (lle mae darparwr gwasanaeth yn storio'ch data ar ei seilwaith) yn golygu bod eich data yn ffisegol ar wahân i'ch lleoliad. Byddwch hefyd yn elwa o lefel uchel o argaeledd. Gall darparwyr gwasanaeth gyflenwi storfa cwmwl i'ch busnes heb fod angen i chi fuddsoddi mewn caledwedd drud ymlaen llaw. Mae'r rhan fwyaf o ddarparwyr yn cynnig swm cyfyngedig o le storio am ddim, a chynhwysedd storio mwy am y costau lleiaf posibl i fusnesau bach.

Cyn cysylltu â darparwyr gwasanaeth, rydym yn eich annog i ddarllen Canllaw Diogelwch Cwmwl yr NCSC. Bydd y canllaw hwn yn eich helpu i benderfynu beth i chwilio amdano wrth werthuso eu gwasanaethau, a beth allant ei gynnig.

Mae meddalwedd wystlo yn aml yn amgryptio copïau wrth gefn ar-lein, sy'n golygu efallai na fydd eich copïau wrth gefn yn y cwmwl ar gael hefyd, gan adael dim copi wrth gefn i chi adfer ohono. I gael mwy o wydnwch, crëwch gopïau wrth gefn all-lein, y mae pwysigrwydd hyn wedi'i gynnwys ym mlog yr NCSC Copïau wrth gefn all-lein mewn byd ar-lein.

Gwnewch greu copi wrth gefn yn rhan o fusnes bob dydd

Gwyddom nad yw gwneud copïau wrth gefn yn beth diddorol iawn i'w wneud (a bydd tasgau pwysicach bob amser y teimlwch y dylid rhoi blaenoriaeth iddynt), ond mae mwyafrif yr atebion storio rhwydwaith neu gymylau bellach yn caniatáu ichi wneud copïau wrth gefn yn awtomatig.

Mae llawer o atebion wrth gefn parod yn hawdd i'w sefydlu, ac yn fforddiadwy o ystyried yr amddiffyniad busnes-gritigol y maent yn ei gynnig. Wrth ddewis datrysiad, bydd yn rhaid i chi hefyd ystyried faint o ddata sydd angen i chi eu gwneud wrth gefn, a pha mor gyflym y mae angen i chi allu cyrchu'r data yn dilyn unrhyw ddigwyddiad.

I gael gwybodaeth fanylach am wneud copïau wrth gefn o'ch data, cyfeiriwch at Ganllaw Busnesau Bach yr NCSC.

Canllawiau seiberddiogelwch

02
Diogelu eich offer swyddfa rhag drwgwedd

Mae drwgwedd yn feddalwedd faleisus, a all - os yw'n gallu rhedeg - achosi niwed mewn llawer o ffyrdd, gan gynnwys:

- achosi i ddyfais gael ei chloi neu fod yn amhosibl i'w defnyddio
- dwyn, dileu neu amgryptio data
- rheoli eich dyfeisiau i ymosod ar fusnesau eraill
- cael manylion mewngofnodi y gellir eu defnyddio i gael mynediad i'ch busnesau (neu wasanaethau a ddefnyddiwch)
- defnyddio gwasanaethau a allai gostio arian i chi (e.e. galwadau ffôn cyfradd premiwm).

Trowch feddalwedd gwrthfeirysau ymlaen

Dylid defnyddio meddalwedd gwrthfeirysau - sy'n aml yn cael ei gynnwys am ddim o fewn systemau gweithredu poblogaidd - ar bob cyfrifiadur a gliniadur. Ar gyfer eich offer swyddfa, mae mor hawdd â chlicio 'galluogi', ac rydych chi'n fwy diogel ar unwaith. Ar gyfer ffonau a thabledi, efallai na fydd angen meddalwedd gwrthfeirysau ar wahân.

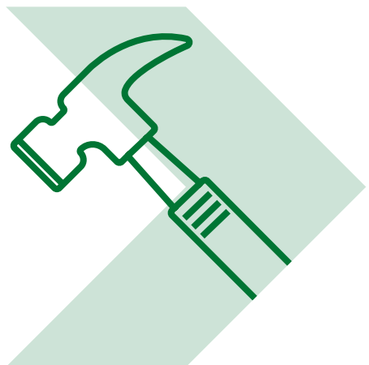
Yn yr un modd, dylech sicrhau bod eich wal dân ymlaen. Mae waliau tân yn creu 'clustogfa' rhwng eich rhwydwaith eich hun a rhwydweithiau allanol (fel y Rhyngrwyd). Mae'r systemau gweithredu mwyaf poblogaidd bellach yn cynnwys wal dân, felly mae'n bosibl mai mater o droi hon ymlaen yw hi.

Lawrlwythwch apiau cymeradwy yn unig

Dim ond o siopau sydd wedi'u cymeradwyo gan y gwneuthurwr (fel Google Play neu Apple App Store) y dylech chi lawrlwytho apiau ar gyfer ffonau symudol a thabledi. Mae'r apiau hyn yn cael eu gwirio i ddarparu lefel benodol o amddiffyniad rhag drwgwedd a allai achosi niwed. Dylech atal staff rhag lawrlwytho apiau trydydd parti o ffynonellau answyddogol, gan na fydd y rhain wedi cael eu gwirio.

Cadwch eich offer TG yn gyfredol

Fel offer pŵer neu beiriannau, mae angen cynnal a chadw a gwasanaethu offer TG (gan gynnwys cyfrifiaduron, gliniaduron, tabledi a ffonau symudol) i sicrhau eu bod yn gweithio'n effeithiol ac yn ddiogel. Mae'r gwaith cynnal a chadw hwn yn cynnwys diweddaru'r meddalwedd y mae'r offer yn rhedeg arno. Ar draws eich holl offer TG, gwnewch yn siŵr bod y system weithredu a meddalwedd gosodedig arall bob amser yn gyfredol â'r fersiynau diweddaraf. Mae cymhwyso'r diweddariadau hyn (proses a elwir yn glytio) yn un o'r pethau pwysicaf y gallwch eu gwneud i wella diogelwch. Dylid gosod dyfeisiau, systemau gweithredu ac apiau i 'ddiweddaru'n awtomatig' lle bynnag y bo hyn yn opsiwn.



Wrth i offer TG gyrraedd diwedd ei oes â chymorth, dylech ei gyfnewid am ddyfais â chymorth. Os byddwch yn parhau i ddefnyddio offer nad yw'n cael ei gefnogi mwyach:

- **ni fydd** yn derbyn diweddariadau sy'n cynnwys nodweddion newydd a gwelliannau perfformiad
- **ni fydd** yn derbyn y diweddariadau diogelwch gan y gwneuthurwr (a heb y rhain mae'ch dyfais yn haws ei hacio)

Trowch amgryptio ymlaen

Sicrhewch fod offer TG eich swyddfa - felly eich gliniaduron a'ch cyfrifiaduron personol - i gyd yn defnyddio cynnyrch amgryptio (fel Bitlocker ar ddyfeisiau Windows, neu FileVault ar gyfer macOS). Mae hyn yn golygu, hyd yn oed os yw'ch cyfrifiadur yn cael ei golli neu ei ddwyn, ni fydd modd cyrchu'r data sydd wedi'i storio arno. I gael cyngor ar ffurfweddu amgryptio disg, cyfeiriwch at ganllawiau Bitlocker a FileVault.

Rheoli sut mae cofau bach USB/cyfryngau symudadwy yn cael eu defnyddio

Mae'n demtasiwn defnyddio gyriannau USB a chardiau SD i drosglwyddo ffeiliau rhwng busnesau a phobl. Fodd bynnag, mae'n hawdd plygio cof bach heintiedig i mewn i ddyfais, dim ond i gyflwyno drwgwedd a allai fod yn niweidiol i'r busnes yn anfwriadol.

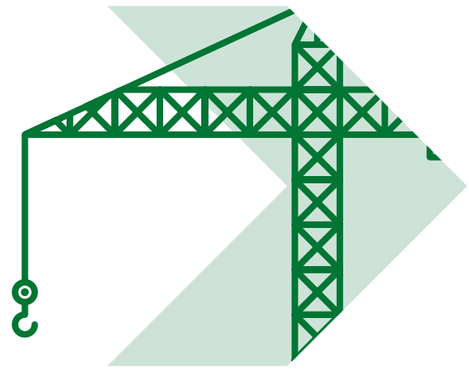
Pan fydd gyriannau a chardiau'n cael eu rhannu'n agored, mae'n dod yn anodd olrhain yr hyn sydd ynddynt, ble maent wedi bod, a phwy sydd wedi'u defnyddio.
Gallwch leihau'r tebygolrwydd o haint drwy:

- rwystro mynediad i borthladdoedd ffisegol ar gyfer y rhan fwyaf o ddefnyddwyr
- defnyddio offer gwrthfeirysau
- dim ond caniatáu i yriannau a chardiau cymeradwy gael eu defnyddio o fewn eich busnes (ac yn unman arall)

Rheoli sut mae trydydd partïon yn cael mynediad i'ch offer TG

Mae'n bosibl y bydd gan sefydliadau ac unigolion y tu allan i'ch busnes resymau dilys dros gael mynediad i'ch offer TG. Efallai bod darparwr gwasanaeth neu ymgynghorydd yn darparu gwasanaethau TG (neu wasanaethau adeiladu) i'ch busnes. Mae angen i chi ddeall sut mae'r mynediad hwn yn cael ei ganiatáu a'i fonitro, a sicrhau mai dim ond yr hyn sy'n ofynnol i gyflawni eu gwaith y gall trydydd partïon ei weld. Wedi'u gadael heb eu rheoli (neu wedi'u gosod yn anghywir), gall troseddwyr fanteisio ar y 'mynediad o bell' hwn i gyflawni ymosodiadau seiber, neu ddwyn gwybodaeth.

I gael gwybodaeth fanylach am amddiffyn eich busnes rhag drwgwedd, cyfeiriwch at Ganllaw Busnesau Bach yr NCSC.



Canllawiau seiberddiogelwch

03
Cadw'ch ffonau a'ch tabledi'n ddiogel

Mae technoleg symudol bellach yn rhan hanfodol o fusnes adeiladu, gyda mwy a mwy yn cael ei ddefnyddio ar safleoedd adeiladu ac wrth symud, gan storio symiau cynyddol o ddata pwysig.
Yn fwy na hynny, mae'r dyfeisiau hyn bellach mor bwerus â chyfrifiaduron traddodiadol, ac oherwydd eu bod yn aml yn gadael diogelwch y swyddfa (a'r cartref), mae angen hyd yn oed mwy o amddiffyniad arnynt nag offer bwrdd gwaith.

Peidiwch â gadael eich ffôn (neu dabled heb ei gloi

Gosodwch gyfrinair clo sgrin, PIN, neu ddull cloi arall (fel olion bysedd neu ddatgloi wyneb). Fel yr eglurwn yng ngham 4, ceisiwch osgoi defnyddio'r cyfrineiriau mwyaf cyffredin (fel '*cyfrinair*').

Sicrhewch y gellir olrhain, cloi neu wagio dyfeisiau sydd ar goll neu wedi'u dwyn

Mae staff yn fwy tebygol o gael eu tabledi neu eu ffonau wedi'u dwyn (neu eu colli) pan fyddant ar y safle. Yn ffodus, mae mwyafrif y dyfeisiau'n cynnwys offer rhad ac am ddim ar y we sy'n amhrisiadwy petaech chi'n colli'ch dyfais. Gallwch eu defnyddio i:

- olrhain lleoliad dyfais
- cloi mynediad i'r ddyfais o bell (i atal unrhyw un arall rhag ei defnyddio)
- dileu o bell y data sydd wedi'u storio ar y ddyfais
- adalw copi wrth gefn o ddata sydd wedi'u storio ar y ddyfais

Cadw dyfeisiau ac apiau yn gyfredol

Yn yr un modd ag offer swyddfa, mae'n bwysig cadw ffonau a thabledi yn gyfredol bob amser. Mae pob gwneuthurwr yn rhyddhau diweddariadau diogelwch rheolaidd i gadw'r ddyfais yn ddiogel. Mae'r broses hon yn gyflym, yn hawdd, ac yn rhad ac am ddim; dylid gosod dyfeisiau i'w diweddaru'n awtomatig, lle bo modd.

Dylai'r holl raglenni rydych chi wedi'u gosod hefyd gael eu diweddaru'n rheolaidd gyda chlytiau gan ddatblygwyr y meddalwedd. Bydd y diweddariadau hyn nid yn unig yn ychwanegu nodweddion newydd, ond byddant hefyd yn trwsio unrhyw dyllau diogelwch a ddarganfuwyd.

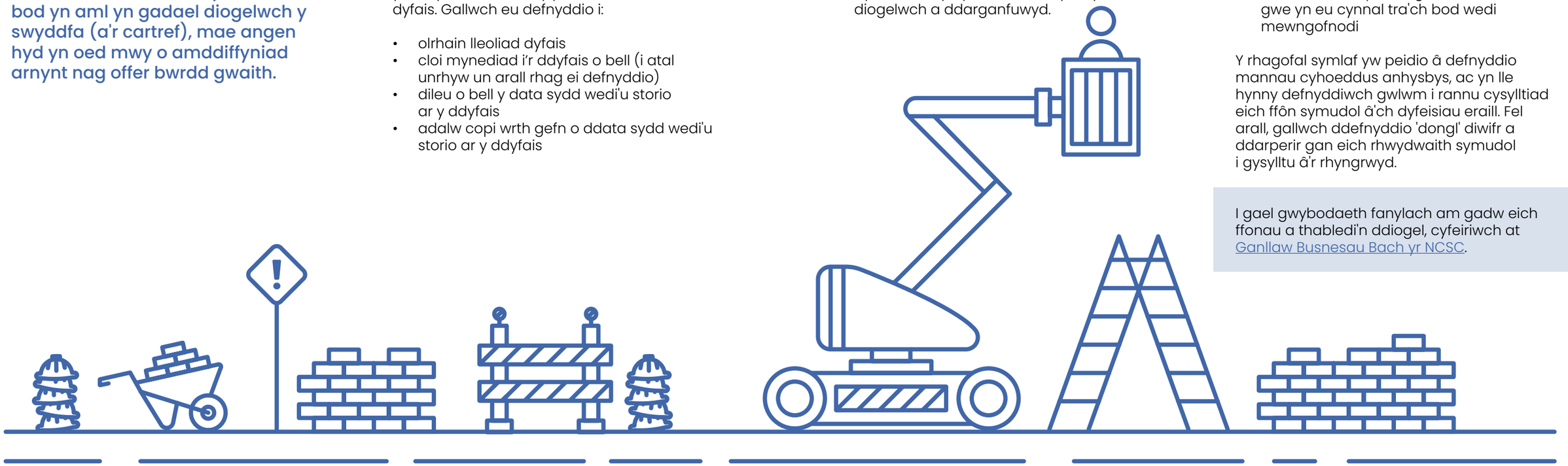
Byddwch yn ofalus wrth gysylltu â mannau Wi-Fi cyhoeddus

Pan fyddwch yn defnyddio mannau Wi-Fi cyhoeddus (er enghraifft mewn gwestai neu siopau coffi), gwnewch yn siŵr eich bod yn cysylltu â gwasanaeth cyfreithlon; bydd aelod o staff yn gallu cadarnhau enw'r gwasanaeth i'w ddefnyddio. Os ydych chi'n cysylltu â 'man cyhoeddus twyllodrus' (hynny yw, man Wi-Fi cyhoeddus a sefydlwyd gan droseddwr seiber), gallent gael mynediad at:

- yr hyn rydych chi'n gweithio arno wrth gysylltu
- eich manylion mewngofnodi preifat y mae llawer o apiau a gwasanaethau gwe yn eu cynnal tra'ch bod wedi mewngofnodi

Y rhagofal symlaf yw peidio â defnyddio mannau cyhoeddus anhysbys, ac yn lle hynny defnyddiwch gwlwm i rannu cysylltiad eich ffôn symudol â'ch dyfeisiau eraill. Fel arall, gallwch ddefnyddio 'dongl' diwifr a ddarperir gan eich rhwydwaith symudol i gysylltu â'r rhyngrwyd.

I gael gwybodaeth fanylach am gadw eich ffonau a thabledi'n ddiogel, cyfeiriwch at Ganllaw Busnesau Bach yr NCSC.



Canllawiau seiberddiogelwch

04
Defnyddio cyfrineiriau i ddiogelu'ch data

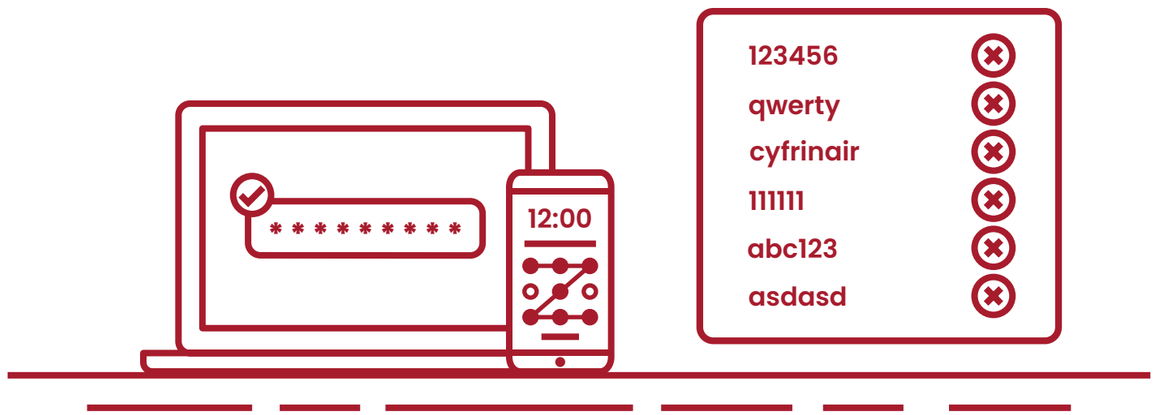
Bydd eich gliniaduron, cyfrifiaduron, tabledi a ffonau yn cynnwys llawer o'ch data busnes-gritigol eich hun, gwybodaeth bersonol eich cwsmeriaid, contractwyr, cyflenwyr, a hefyd manylion y cyfrifon ar-lein rydych chi'n eu defnyddio. Mae cyfrineiriau - pan gânt eu gweithredu'n gywir - yn ffordd rad ac am ddim, hawdd ac fel arfer yn effeithiol i atal pobl heb awdurdod rhag cael mynediad i'ch dyfeisiau. Mae gan yr NCSC gyngor defnyddiol ar sut i ddewis cyfrinair anrhagweladwy y gallwch ei gofio.

Cofiwch droi amddiffyniad cyfrinair ymlaen

Gosodwch gyfrinair clo sgrin, PIN, neu ddull cloi arall (fel olion bysedd neu ddatgloi wyneb). Bydd angen i chi osod cyfrinair ar y rhan fwyaf o ddyfeisiau pan fyddwch yn eu defnyddio am y tro cyntaf, ond efallai y bydd rhywun arall wedi'i ddiffodd.

Osgowch ddefnyddio cyfrineiriau rhagweladwy

Dylai cyfrineiriau fod yn hawdd i'w cofio, ond yn anodd i rywun arall eu dyfalu. Rheol dda yw 'gwnewch yn siŵr bod rhywun sy'n eich adnabod yn dda yn methu â dyfalu'ch cyfrinair mewn 20 ymgais'. Dylai staff hefyd osgoi defnyddio'r cyfrineiriau mwyaf cyffredin (fel '*cyfrinair*'), y mae troseddwyr yn eu defnyddio i gael mynediad cryfach i'ch cyfrif, neu rai y gallai rhywun eu dyfalu o'ch proffil cyfryngau cymdeithasol (felly osgowchd defnyddio enwau teulu, enw anifail anwes, lleoliad geni, neu rywbeth yn ymwneud â hoff dîm chwaraeon).



Mae'n bwysig iawn peidio ag ailddefnyddio'r un cyfrinair ar gyfer eich gwahanol gyfrifon ar-lein. Yn benodol, defnyddiwch gyfrinair cryf a gwahanol ar gyfer eich e-bost. Os gall haciwr gael mynediad i'ch blwch derbyn, gall gael mynediad at wybodaeth am eich taliadau, anfonebau, contractwyr a chyflenwyr), yn ogystal ag anfon e-byst yn esgus eu bod oddi wrthych.

Defnyddiwch 2FA ar gyfer cyfrifon pwysig

Os ydych yn cael y dewis i ddefnyddio dilysu dau-ffactor (a elwir hefyd yn 2FA) ar gyfer unrhyw gyfrifon dylech, ac yn enwedig ar gyfer **e-bost**, **bancio** a **phrynu**. Mae hyn yn ychwanegu llawer iawn o ddiogelwch am ddim llawer o ymdrech ychwanegol. Mae 2FA angen dau ddull gwahanol i 'brofi' pwy ydych chi cyn y gallwch ddefnyddio gwasanaeth, yn gyffredinol rhywbeth rydych chi'n ei *wybod* (fel cyfrinair) a rhywbeth sydd *gennych* chi (fel ffôn). Gallai hwn fod yn god sy'n cael ei anfon i'ch ffôn (neu god a gynhyrchir gan ddarllenydd cerdyn banc) y mae'n rhaid i chi ei nodi yn ogystal â'ch cyfrinair.

Gofalu am eich cyfrineiriau

Wrth gwrs mae gan y rhan fwyaf ohonom *lawer* o gyfrifon ar-lein, felly mae creu cyfrineiriau gwahanol ar gyfer pob un ohonynt (a'u cofio) yn anodd. Fodd bynnag, i wneud hyn yn haws, gallwch:

1. Ysgrifennu'ch holl gyfrineiriau ar ddarn o bapur a'i gadw yn rhywle diogel (ac **i ffwrdd** o'ch cyfrifiadur).

2. Gadewch i'ch porwr gadw eich cyfrineiriau i chi - **mae'n ddiogel i chi eu cadw pan ofynnir i chi**, (er os ydych chi'n rhannu'ch cyfrifiadur ag unrhyw un, byddan nhw hefyd yn gallu cyrchu'r cyfrifon).

Gallwch hefyd ddefnyddio rheolwr cyfrineiriau, sy'n gallu creu a storio cyfrineiriau i chi y byddwch yn eu cyrchu trwy gyfrinair 'feistr'.

Os oes mwy nag un person yn defnyddio cyfrifiadur, yn ddelfrydol dylai fod gennych gyfrifon gwahanol, a chyfrineiriau gwahanol ar gyfer pob person. Lle nad yw hyn yn bosibl, gwnewch yn siŵr eich bod yn gwybod **pwy** sydd â mynediad i'ch dyfeisiau, pwy sy'n gwybod y cyfrinair, a'ch bod yn hapus â hyn. Peidiwch ag ysgrifennu'r cyfrinair ar nodyn gludiog sy'n sownd wrth y cyfrifiadur, i unrhyw un ei ddefnyddio. Am yr un rhesymau, clowch eich dyfais pan nad ydych wrth eich desg, a gwnewch yn siŵr eich bod yn newid eich cyfrineiriau pan fydd aelod o staff sydd â mynediad i'ch dyfeisiau yn gadael.

Newid pob cyfrinair rhagosodedig

Yn olaf, un o'r camgymeriadau mwyaf cyffredin yw peidio newid cyfrineiriau rhagosodedig y gwneuthurwyr a roddir i ffonau, gliniaduron a mathau eraill o offer. Gellir dod o hyd i'r rhain yn hawdd ar-lein. Newidiwch yr holl gyfrineiriau rhagosodedig cyn i ddyfeisiau gael eu dosbarthu i staff.

I gael gwybodaeth fanylach am ddefnyddio cyfrineiriau i ddiogelu eich data a dyfeisiau, cyfeiriwch at Ganllaw Busnesau Bach yr NCSC.

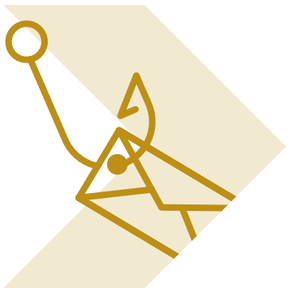
Canllawiau seiberddiogelwch

05
Delio â gwe-rwydo

'Gwe-rwydo' yw pan fydd troseddwyr yn defnyddio e-byst, negeseuon SMS neu sgwrsio twyllodrus, galwadau ffôn neu gyfryngau cymdeithasol i dwyllo eu dioddefwyr.

Eu nod yn aml yw eich argyhoeddi i glicio ar ddolen, neu agor atodiad. Unwaith y bydd rhywun wedi clicio (neu agor), gellir gosod meddalwedd maleisus trwy wefan amheus yr ydych wedi cael eich anfon ati, neu drwy'r atodiad yr ydych wedi'i agor. Dros y ffôn, efallai y bydd y dull gweithredu yn fwy uniongyrchol, gan ofyn i chi am wybodaeth sensitif, fel manylion banc.

Mae'n bosibl y bydd rhai troseddwyr hyd yn oed yn anfon neges sgam mwy *targedig* (proses a elwir yn we-drywanu), sy'n cymryd arnynt eu bod gan gwmni cyfreithlon yr ydych yn delio ag ef. Mae'r ymosodiadau mwy targedig hyn yn edrych fe petaent yn dod o ffynonellau mwy cyfreithlon, ac yn cael eu hanfon at uwch staff neu ddeiliaid cyllidebau o fewn busnesau mwy, a allai fod â mynediad at gyllid a gwybodaeth fwy gwerthfawr. Yn wahanol i negeseuon gwe-rwydo safonol sy'n cael eu hanfon yn ddiwahân i filiynau o bobl, mae ymosodiadau gwe-drywanu wedi'u llunio i apelio at unigolion penodol, a gallant fod yn anoddach fyth i'w canfod. Mae gwe-rwydo (a gwe-drywanu) yn fygythiad i bob busnes o bob maint ac ar draws pob sector, gan gynnwys adeiladu.



Rhoi gwybod am e-byst, negeseuon testun, gwefannau sgam i'r iNCSC

Os ydych chi neu aelod o staff sydd wedi derbyn e-bost nad ydych yn hollol siŵr amdano, anfonwch ef ymlaen at Wasanaeth Adrodd E-bost Amheus (SERS) yr NCSC yn report@phishing.gov.uk Dylid anfon negeseuon testun amheus ymlaen at 7726 – mae'n rhad ac am ddim.

Gwnewch eich hun yn darged anoddach

Gall troseddwyr ddefnyddio gwybodaeth amdanoch y gellir ei gweld yn hawdd ar eich gwaith a gwefannau preifat (gan gynnwys cyfrifon cyfryngau cymdeithasol) i wneud i'w negeseuon gwe-rwydo ymddangos yn fwy argyhoeddiadol. Adolygwch eich gosodiadau preifatrwydd, a meddyliwch am yr hyn rydych chi'n ei bostio ar draws eich cyfrifon cymdeithasol a phroffesiynol. Byddwch yn ymwybodol o'r hyn y mae eich ffrindiau, eich teulu a'ch cydweithwyr yn ei ddweud amdanoch ar-lein, oherwydd gall hyn hefyd ddatgelu gwybodaeth y gellir ei defnyddio i'ch targedu.

Meddyliwch am sut rydych chi'n gweithredu

Ystyriwch ffyrdd y gallai rhywun dargedu eich busnes, a gwnewch yn siŵr bod eich holl staff yn deall ffyrdd arferol o weithio (yn enwedig o ran rhyngweithio â busnesau eraill), fel eu bod mewn gwell sefyllfa i sylwi ar geisiadau sy'n anarferol. Mae triciau cyffredin mewn adeiladu yn cynnwys twyllo staff i drosglwyddo arian neu wybodaeth trwy anfon e-byst sy'n edrych yn ddilys. Un arall yw anfon anfoneb am wasanaeth nad ydych wedi'i ddefnyddio, felly pan fydd yr atodiad yn cael ei agor, mae drwgwedd yn cael ei osod yn awtomatig (yn ddiarwybod i chi) ar y cyfrifiadur.

Meddyliwch am eich arferion gwaith cyffredinol a sut y gallwch chi helpu i wneud y triciau hyn yn llai tebygol o lwyddo. Er enghraifft:

- A yw staff yn gwybod beth i'w wneud â cheisiadau anarferol, a ble i gael cymorth?
- Gofynnwch i chi'ch hun a ddylai rhywun sy'n dynwared unigolyn pwysig (cwsmer neu reolwr) trwy e-bost gael ei herio (neu gael dilysu ei hunaniaeth mewn ffordd arall) cyn cymryd camau.
- Meddyliwch am sut y gallwch chi annog a chefnogi eich staff i gwestiynu ceisiadau amheus neu anarferol – hyd yn oed os yw'n ymddangos eu bod gan unigolion pwysig. Gall bod â'r hyder i ofyn 'a yw hyn yn ddilys?' fod y gwahaniaeth rhwng aros yn ddiogel, neu anffawd gostus.

Gwiriwch am arwyddion amlwg gwe-rwydo

Mae sgamwyr yn gobeithio ennill eich ymddiriedaeth yn gyflym a'ch perswadio neu roi pwysau arnoch i weithredu heb feddwl. Yn aml bydd gan negeseuon sgam un neu fwy o'r 5 arwydd canlynol.

1. **Awdurdod** - A yw'r neges yn honni ei bod yn dod oddi wrth rywun swyddogol neu sefydliad yr ydych yn gweithio'n agos ag ef? Er enghraifft, eich banc, cleientiaid, cyflenwyr, neu awdurdod lleol. Mae troseddwyr yn aml yn cymryd arnynt eu bod yn bobl neu'n sefydliadau pwysig i'ch twyllo i wneud yr hyn y maent ei eisiau.

2. **Brys** - A ddywedir wrthych fod gennych amser cyfyngedig i ymateb ('o fewn 24 awr' neu 'ar unwaith' er enghraifft)? Mae troseddwyr yn aml yn eich bygwth â dirwyon neu ganlyniadau negyddol eraill.

3. **Emosiwn** - A oes gan y neges naws a all wneud i weithwyr deimlo panig, yn ofnus, yn obeithiol neu'n chwilfrydig? Mae troseddwyr yn aml yn defnyddio iaith fygythiol, yn gwneud honiadau ffug o gefnogaeth, neu'n eich pryfocio i fod eisiau darganfod mwy.

4. **Prinder** - A yw'r neges yn cynnig rhywbeth prin, fel deunyddiau, offer neu feddalwedd? Gall ofn colli allan ar fargen dda neu gyfle wneud i bobl ymateb yn gyflym.

5. **Digwyddiadau cyfredol** - Ydych chi'n disgwyl gweld neges fel hon? Mae troseddwyr yn aml yn ecsbloetio eich perthynas â chleientiaid a chyflenwyr i'ch twyllo i dalu symiau o arian a hefyd yn defnyddio adegau penodol o'r flwyddyn (fel adrodd treth) i wneud i'w sgam ymddangos yn fwy perthnasol i chi.

Beth i'w wneud os ydych eisoes wedi clicio

Os ydych wedi colli arian neu wedi cael eich hacio o ganlyniad i ymateb i neges gwe-rwydo, dylech roi gwybod amdano:

- Yng Nghymru, Lloegr neu Ogledd Iwerddon, ewch i www.actionfraud.police.uk neu ffoniwch **0300 123 2040**.
- Yn yr Alban, riportiwch i Heddlu'r Alban drwy ffonio **101**.
- Efallai y bydd eich banc hefyd yn gallu helpu os ydych yn meddwl eich bod wedi cael eich twyllo i drosglwyddo arian i droseddwr.

Canllawiau seiberddiogelwch

06
Cydweithio â chyflenwyr a phartneriaid

Mae busnesau adeiladu'n dibynnu ar gyflenwyr i ddosbarthu deunyddiau, peiriannau, llafur a gwybodaeth ddigidol (fel manylebau a dyluniadau). Hyd yn oed ar gyfer busnesau llai, gall eich cadwyn gyflenwi ddod yn fawr a chymhleth yn gyflym, gan gynnwys defnydd helaeth o isgontractwyr a chyflenwyr gyda lefel uchel o daliadau yn llifo i ac o fusnesau.

Yna mae yna sefydliadau llai amlwg yr ydych yn dibynnu arnynt. Er enghraifft darparwr eich gwasanaeth e-bost, neu'r cwmni y tu ôl i'r meddalwedd cyfrifo rydych chi'n ei ddefnyddio.

Gall ymosodiadau seiber ar eich cyflenwyr fod yr un mor niweidiol ag ymosodiad ar eich busnes eich hun. Dyna pam ei bod yn bwysig defnyddio seiberddiogelwch wrth gydweithio â chyflenwyr a phartneriaid. Efallai y cewch eich targedu fel ffordd i mewn i'r sefydliad yr ydych yn ei gyflenwi. Mae hyn yn gyffredin iawn yn y diwydiant adeiladu, oherwydd efallai eich bod eisoes yn gweithio gyda sefydliadau y mae'r ymosodwr am gael mynediad iddynt drwoch chi.

I'r gwrthwyneb, efallai y bydd eich cyflenwyr yn cael eu targedu fel llwybr i mewn i'ch busnes. Neu efallai eich bod yn rhannu gwybodaeth sensitif neu werthfawr yr ydych am i gyflenwyr ei diogelu.

Efallai y bydd busnesau adeiladu hefyd am annog eu cyflenwyr i gael ardystiad Hanfodion Seiber. Mae Hanfodion Seiber yn gynllun a gefnogir gan y llywodraeth, gyda nawdd gan y diwydiant i helpu sefydliadau i amddiffyn eu hunain rhag ymosodiadau seiber cyffredin. Mae sefydliadau sydd ag ardystiad Hanfodion Seiber wedi dangos eu bod yn cymryd seiberddiogelwch o ddifrif, a gallant ddefnyddio'r sicrwydd hwn i ddenu busnes newydd a rhoi sicrwydd i'w cwsmeriaid.

Deall eich cadwyn gyflenwi

Hyd nes y bydd gennych ddarlun clir o'ch cadwyn gyflenwi bresennol, bydd yn anodd iawn penderfynu sut i'w diogelu. Sicrhewch fod gennych restr o'ch holl gyflenwyr, a phartneriaid, a nodwch pa rai sydd â'r flaenoriaeth uchaf (o ran risg) i ganolbwyntio'ch ymdrechion arnynt. Lle bo modd, cynhwyswch isgontractwyr sy'n dechrau gyda'ch cyflenwyr uniongyrchol â'r flaenoriaeth uchaf.

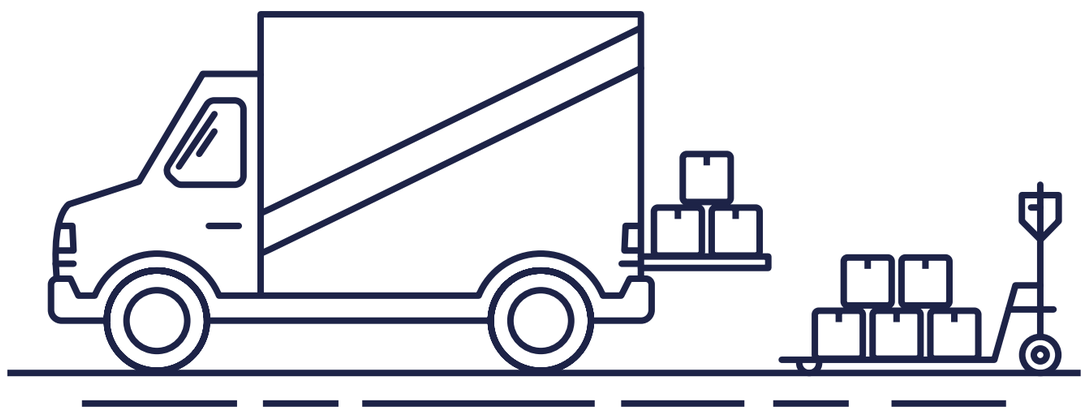
Chwiliwch am wybodaeth a gyhoeddir gan eich cyflenwyr presennol sy'n eich helpu i ddeall sut maent yn darparu gwasanaethau'n ddiogel. Sicrhewch eich bod yn deall y telerau ac amodau yn eich contract neu gytundeb trwyddedu, a pha rannau o ddiogelwch y mae pob un yn gyfrifol amdanynt. Bydd hyn yn eich helpu i ddatblygu dealltwriaeth gyffredin o gyfrifoldebau diogelwch pob parti, a pha benderfyniadau is-gontractio yr ydych yn fodlon eu dirprwyo iddynt. Gallai fod yn ddefnyddiol cynnwys cyfeiriadau at ganllawiau canlynol NCSC a all helpu sefydlu gwaelodlin o seiberddiogelwch:

- 10 Cam at Seiberddiogelwch
- Canllaw i Fusnesau Bach
- Hanfodion Seiber

Ystyriwch y goblygiadau os bydd rhywun yn ymosod ar eich cyflenwr

Waeth pa mor dda yw eich seiberddiogelwch eich hun, dylech gymryd yn ganiataol y **byddwch** chi a'ch partneriaid yn profi digwyddiad seiber rywbryd, a chynllunio ar gyfer hynny. Mae hyn hefyd yn werth ei ystyried yn eich cytundebau diogelwch; beth ydych chi'n ei ddisgwyl ganddyn nhw a'u hymateb? Oes rhaid iddyn nhw roi gwybod i chi? A oes rhaid iddynt eich cynorthwyo os bydd rhywun yn ymosod arnoch hefyd o ganlyniad?

I gael gwybodaeth fanylach am gydweithio â chyflenwyr a phartneriaid, ewch i'r adran cadwyn gyflenwi yng nghanllaw Pecyn Cymorth Bwrdd yr NCSC.



Canllawiau seiberddiogelwch

07
Paratoi ar gyfer (ac ymateb i) ddigwyddiadau seiber

Pan fydd rhywbeth annisgwyl yn digwydd, fel digwyddiad seiber, gall fod yn anodd gwybod sut i ymateb. Yn naturiol, byddwch am ddatrys y broblem cyn gynted â phosibl fel y gallwch ailddechrau busnes yn gyflym. Mae drwgwedd (ac yn enwedig meddalwedd wystlo) yn dod yn fwyfwy cyffredin yn y diwydiant adeiladu, felly mae'n hanfodol bod yn barod.

Mae'n anymarferol datblygu cyfarwyddiadau cam-wrth-gam manwl i reoli pob math o ddigwyddiad, gan y gallai'r rhestr fod yn ddiddiwedd. Yn hytrach, dylech baratoi cynlluniau i ymdrin â'r digwyddiadau hynny sydd fwyaf tebygol o ddigwydd.

Y ffordd orau o brofi dealltwriaeth eich staff o'r hyn sydd ei angen yn ystod digwyddiad yw drwy ymarfer seiber, sy'n cynnwys ymarfer eich ymateb i ddigwyddiad seiber. Ystyriwch ddefnyddio cynnyrch Ymarfer mewn Blwch yr NCSC, sydd wedi'i gynllunio'n arbennig ar gyfer sefydliadau llai, i brofi gwydnwch a pharodrwydd eich busnes.

Paratoi ar gyfer digwyddiadau

Nodwch ba **wybodaeth electronig** sy'n hanfodol i gadw'ch busnes i redeg, megis manylion cyswllt a chyflenwyr, e-byst, anfonebau, a dogfennau hanfodol. Darganfyddwch ble mae'r wybodaeth hon yn cael ei storio. A yw ar un peiriant yn eich swyddfa? Ai ar weinydd pell? A yw'n cael ei storio yn y cwmwl, neu gan drydydd parti?

Gwnewch yn siŵr eich bod yn cadw'r wybodaeth bwysig a nodwyd gennych uchod mewn man diogel fel y gallwch ei defnyddio os caiff eich offer ei ddwyn neu ei ddifrodi gan ymosodiad seiber. Sicrhewch eich bod yn gwybod sut i adfer copi wrth gefn os bydd unrhyw fath o ddata'n cael eu colli, fel ymosodiad meddalwedd wystlo, a hyfforddwch y bobl berthnasol yn eich busnes fel y gallant wneud yr un peth. Gallai bod yn barod a chael dogfennau perthnasol sy'n gyfredol ac sydd hefyd yn **hygyrch** pan fydd digwyddiad yn digwydd gwneud byd o wahaniaeth.

Os oes gennych chi yswiriant seiber, gwnewch yn siŵr bod manylion eich yswiriwr wedi'u cofnodi, gan gynnwys rhif y polisi ac unrhyw wybodaeth benodol y mae eich darparwr yn gofyn amdani. Sicrhewch eich bod yn deall unrhyw gydymffurfiaeth gyfreithiol neu reoleiddiol y mae'n rhaid i chi gadw atynt a gweithredu unrhyw ganllawiau/polisïau/rheolau y maent yn eu gosod ar eich cyfer. Dylech wirio a oes gan eich cymdeithas fasnach neu gorff proffesiynol unrhyw gymorth neu linellau cyngor y gallwch gysylltu â nhw i'ch helpu yn y sefyllfa hon.

Nodi a oes rhywun yn ymosod arnoch

Mae'r cam cyntaf wrth ddelio'n effeithiol â digwyddiad seiber yn cynnwys ei adnabod. Hynny yw, sut allwch chi ganfod bod digwyddiad wedi digwydd (neu'n dal i ddigwydd)?

Ymhlith y pethau a allai fod yn arwydd o ddigwyddiad seiber mae:

- negeseuon yn mynnu gwystl ar gyfer rhyddhau eich ffeiliau
- cyfrifiaduron yn rhedeg yn araf
- defnyddwyr yn cael eu cloi allan o'u cyfrifon
- defnyddwyr yn methu cael mynediad at ddogfennau
- pobl yn eich hysbysu eu bod wedi derbyn e-byst anarferol gennych
- chwiliadau rhyngrwyd wedi'u hailgyfeirio
- ceisiadau am daliadau anawdurdodedig
- gweithgaredd cyfrif anarferol

I helpu gyda hyn, gallwch ddefnyddio teclyn Cofnodi Hwylus yr NCSC, sydd wedi'i gynllunio'n benodol i helpu busnesau bach sydd heb y gyllideb, yr amser na'r ddealltwriaeth i sefydlu eu system cofnodi eu hunain.

Gall eich meddalwedd gwrthfeirysau hefyd ddarparu dangosyddion perygl i chi; cyflawnwch sgan llawn a dadansoddi'r canlyniadau i weld a yw wedi canfod unrhyw ddrwgwedd. Mae cyngor ar beth i'w wneud fel arfer ar gael ar wefan y cwmni gwrthfeirysau

(parhad ar y dudalen nesaf)

Canllawiau seiberddiogelwch

Datrys y digwyddiad

Bydd y camau gweithredu yn y cam hwn yn helpu'ch busnes i ailddechrau cyn gynted â phosibl. Bydd angen i chi hefyd gadarnhau bod popeth yn gweithio'n normal, a thrwsio unrhyw broblemau.

Os caiff eich TG ei reoli'n allanol, cysylltwch â'r bobl gywir i helpu. Mae'r cysylltiadau hyn yno i ddatrys y broblem a sefydlu'r effaith ar eich busnes.

Os ydych yn rheoli eich TG eich hun, rhowch y cynlluniau a wnaethoch yn gynharach ar waith. Yn dibynnu ar y math o ddigwyddiad yr ydych yn ymateb iddo, gall hyn gynnwys:

- amnewid caledwedd sydd dan fygythiad
- adfer gwasanaethau trwy gopïau wrth gefn
- meddalwedd clytio
- glanhau peiriannau heintiedig
- newid cyfrineiriau

Gallech ddefnyddio cwmni yng nghynllun Ymateb i Ddigwyddiad Seiber (CIR) yr NCSC os oedd eich sefydliad yn ddioddefwr ymosodiad seiber sylweddol. Byddai'r cwmni sydd wedi'i ardystio gan CIR yn cynnal yr holl weithgareddau ymateb i ddigwyddiadau seiber mewn perthynas â'r ymosodiad i helpu'ch sefydliad i adfer.

Sylwch fod rhwymedigaeth gyfreithiol arnoch i adrodd am ddigwyddiadau penodol (fel toriad data) i Swyddfa'r Comisiynydd Gwybodaeth (ICO), p'un a yw eich TG wedi'i allanoli ai peidio. Edrychwch ar wefan yr ICO i weld ar gyfer pa ddigwyddiadau mae hyn yn ofynnol. Mae'n bosibl y bydd cyrff rheoleiddio eraill yr ydych yn perthyn iddynt hefyd yn mynnu eich bod yn adrodd am doriad.

Dysgu o'r digwyddiad

Ar ôl y digwyddiad, mae'n bwysig adolygu'r hyn sydd wedi digwydd, dysgu o unrhyw gamgymeriadau, cymryd camau i geisio lleihau'r tebygolrwydd y bydd yn digwydd eto. I wneud hyn:

1. Adolygwch y camau a gymerwyd yn ystod eich ymateb. Gwnewch restr o'r pethau a aeth yn dda a'r pethau y gellid eu gwella o'r cam ymateb.

2. Adolygwch a diweddarwch eich cynllun digwyddiad, a lle bo angen, gwnewch newidiadau i'r cynllun digwyddiad a grëwyd gennych, i adlewyrchu'r gwersi a ddysgwyd.

3. Cryfhewch eich amddiffynfeydd trwy wneud unrhyw newidiadau angenrheidiol.

Er enghraifft, os oeddech wedi dioddef ymosodiad cyfrinair, efallai y bydd angen i chi greu polisi cyfrinair newydd.

I gael gwybodaeth fanylach am baratoi ar gyfer digwyddiadau, cyfeiriwch at Ganllaw Busnesau Bach i Ymateb ac Adfer yr NCSC.

Ble i fynd am ragor o gymorth

Os byddwch yn derbyn neges gwe-rwydo bosibl, gallwch ei riportio i'r NCSC gan ddefnyddio'r Gwasanaeth Adrodd E-bost Amheus (SERS). Anfonwch y neges ymlaen at report@phishing.gov.uk. Os canfyddir bod y neges yn cysylltu â chynnwys maleisus, bydd yn cael ei thynnu i lawr neu ei rhwystro, gan helpu i atal dioddefwyr trosedd yn y dyfodol.

Dylid anfon negeseuon testun amheus ymlaen i 7726. Mae'r cod byr rhad ac am ddim hwn yn galluogi eich darparwr i ymchwilio i darddiad y neges ac i gymryd camau, os canfyddir ei fod yn faleisus.

Os bydd eich busnes yn dioddef digwyddiad seiber neu'n cael ei effeithio gan dwyll (e.e. arian a gollwyd o ganlyniad i e-bost gwe-rwydo neu os yw eich systemau TG wedi'u peryglu), rhowch wybod i Action Fraud drwy ffonio 0300 123 2040 neu ewch i www.actionfraud.police.uk, neu yn yr Alban trwy ganolfan alwadau 101 Heddlu'r Alban.

Os ydych yn chwilio am gyngor ar ddiogelwch asedau adeiledig a thir y cyhoedd, gall aelodau o'r Gofrestr Peirianwyr ac Arbenigwyr Diogelwch (RSES) a noddir gan CPNI ddarparu cyngor neu arweiniad penodol, gan gynnwys diogelwch systemau digidol yn yr amgylchedd adeiledig.

Os hoffech ragor o wybodaeth a chyngor ar faterion diogelwch corfforol neu bersonél neu feddylfryd diogelwch, gan gynnwys asesu risg, diogelwch safle, cynhyrchion diogelwch achrededig a rheoli gwybodaeth, cyfeiriwch at wefan y CPNI yn www.cpni.gov.uk.

National Cyber Security Centre
a part of GCHQ

Am ragor o wybodaeth, neu i gysylltu â ni, ewch i: **www.ncsc.gov.uk**

@NCSC

Y Ganolfan Seiberddiogelwch Genedlaethol

@cyberhq

Gwybodaeth yn gywir ar adeg cyhoeddi - **Ionawr 2022**

Dyluniwyd a chrëwyd gan Agent Marketing Ltd.
agentmarketing.co.uk