Canllawiau i ganolfannau ar seiberddiogelwch

Cyflwyniad

Mae cyrff dyfarnu wedi ymrwymo i gynnal y safonau seiberddiogelwch uchaf er mwyn ddiogelu gwybodaeth sensitif a ddarperir gan ganolfannau, gan gynnwys data personol myfyrwyr, ac i ddiogelu uniondeb asesiadau diogel. Mae gan ganolfannau a staff canolfannau rôl hanfodol o ran cynnal a gwella seiberddiogelwch.

Ym myd ddigidol heddiw, mae'n hanfodol bod canolfannau'n cadw at arferion gorau'r diwydiant i liniaru'r risg o fygythiadau seiber. Mae'r ddogfen hon yn darparu canllawiau allweddol sy'n cyd-fynd â safonau'r diwydiant i helpu canolfannau a staff canolfannau i ddiogelu eu hasedau digidol.

Arferion gorau rheoli cyfrifon

Dyma rhywfaint o ganllawiau hanfodol ar gyfer rheoli cyfrifon defnyddwyr yn ddiogel. Dylid dilyn y canllawiau hyn ar gyfer holl gyfrifon defnyddwyr/e-bost y corff dyfarnu a ddefnyddir i ddarparu neu reoli mynediad i systemau, gwybodaeth neu ddata'r corff dyfarnu. Trwy ddilyn yr arferion gorau hyn, gall canolfannau a staff canolfannau leihau'n sylweddol y risg o fynediad heb awdurdod a diogelu gwybodaeth sensitif ac asedau gwerthfawr eraill.

Creu cyfrineiriau unigryw cryf

- Defnyddiwch ddull creu cyfrinair fel tri gair ar hap i gynhyrchu cyfrineiriau diogel addas.

  Mae ymchwil yn dangos bod hyd cyfrinair yn amddiffyniad mwy gwerthfawr na chymhlethdod.

- Peidiwch byth â defnyddio gwybodaeth hawdd ei dyfalu fel penblwyddi, enwau unigol neu eiriau cyffredin ar gyfer cyfrinair.

  Gall ymosodwyr ddarganfod y rhain yn hawdd a byddant yn aml yn ceisio darganfod y math hwn o wybodaeth.

- Defnyddiwch gyfrinair unigryw cryf ar gyfer pob cyfrif a ddefnyddir a pheidiwch byth â defnyddio'r un cyfrinair ar draws unrhyw gyfrif arall.

  Pan gaiff cyfrineiriau eu hailddefnyddio, mae torri diogelwch un cyfrif yn peryglu pob cyfrif sydd â'r un cyfrinair a rennir. Mae ymosodwyr yn aml yn defnyddio rhestrau e-bost a chyfrineiriau sydd wedi'u torri i geisio cael mynediad at wasanaethau eraill.

Cadwch holl fanylion y cyfrif yn gyfrinachol

- Peidiwch byth â rhannu manylion mewngofnodi/cyfrinair na chodau ffactor/dilysu ychwanegol gydag unrhyw un arall.

  Bydd ymosodwyr yn aml yn ceisio twyllo pobl i rannu'r manylion hynny gyda nhw drwy esgus eu bod yn dod o'u corff dyfarnu, tîm cefnogaeth technegol neu sefydliad arall.

- Dylai pob person sydd angen mynediad at system ofyn am ei gyfrif defnyddiwr ei hunain a pheidio byth â rhannu cyfrif a neilltuwyd i'w ddefnyddio gydag unrhyw un arall.

Cofiwch y bydd unrhyw beth a wneir gyda chyfrif a neilltuwyd i rywun yn cael ei briodoli i'r person hwnnw yn y lle cyntaf.

Galluogi gosodiadau diogelwch ychwanegol lle bynnag y bo modd

- Actifadu dilysu dau gam (2SV)/dilysu dau ffactor (2FA) neu ddilysu aml-ffactor (MFA) lle bynnag y mae ar gael. Mae gwneud hyn yn ychwanegu haen o ddiogelwch i'r cyfrif sy'n ei gwneud yn ofynnol i ddefnyddwyr gymryd camau ychwanegol neu ddarparu gwiriad ychwanegol fel olion bysedd, cod neu gadarnhau trwy ap dilysu.

  Mae 2SV/2FA/MFA ond yn helpu i amddiffyn defnyddwyr os yw'r camau/ffactorau ychwanegol yn cael eu diogelu. Bydd ymosodwyr yn ceisio twyllo defnyddwyr i roi codau mynediad/rhannu, felly mae angen cadw'r ffactorau hyn mor ddiogel â chyfrineiriau.

Diweddaru unrhyw gyfrineiriau a allai fod wedi cael eu datgelu

- Os credir bod cyfrineiriau wedi cael eu datgelu / dod yn hysbys i eraill, dylid eu newid cyn gynted â phosibl. Ni ddylid rhannu'r cyfrineiriau newydd gydag unrhyw un.

- Wrth newid cyfrineiriau, dylid defnyddio cyfrineiriau unigryw cryf (e.e. tri gair ar hap) bob amser. Ni ddylid ailddefnyddio hen gyfrineiriau ac ni ddylid cylchu drwy set bach o gyfrineiriau ar draws sawl cyfrif.

  Pan fydd cyfrineiriau yn cael eu hailddefnyddio, neu'n dilyn patrwm amlwg, mae gan ymosodwyr offer a fydd yn eu helpu i nodi patrymau ailddefnyddio / patrymau cylchu.

Sefydlu opsiynau adfer cyfrifon diogel

- Dylid sefydlu neu gadw opsiynau adfer cyfrifon wedi'u diweddaru megis cyfrifon e-bost neu rifau ffôn bob yn ail i hwyluso mynediad i gyfrifon mewn achos o gloi allan neu gyfaddawd.

  Bydd ymosodwyr yn ceisio defnyddio opsiynau adfer cyfrifon (e.e. cyfrif e-bost arall a nodwyd fel y cyfrif adfer) i gymryd cyfrif drosodd, felly lle bynnag y bo modd dylid galluogi diogelwch 2SV / 2FA / MFA ar bob cyfrif o'r fath i sicrhau eu bod yn aros yn ddiogel rhag hacwyr.

Adolygu a rheoli ceisiadau cysylltiedig

- Adolygu a dileu mynediad yn rheolaidd ar gyfer cymwysiadau neu wasanaethau trydydd parti nad oes angen mynediad i gyfrifon arnynt mwyach.

  Gall ymosodwyr dorri diogelwch gwasanaethau y rhoddwyd mynediad iddynt i ddefnyddwyr ac yna defnyddio'r mynediad hwnnw i geisio cyrchu cyfrifon y defnyddiwr. Dylid darparu mynediad i wasanaethau dibynadwy yn unig. Dylai staff canolfannau fod yn arbennig o ofalus wrth ryngweithio â chynnwys a gwasanaethau (e.e. cwisiau, ennill gwobr, arolygon ac ati) ar lwyfannau cyfryngau cymdeithasol gan fod y rhain yn aml yn cael eu defnyddio gan ymosodwyr i gael mynediad at wybodaeth defnyddwyr.

- Byddwch yn ofalus wrth roi caniatâd i geisiadau a dim ond rhoi'r mynediad angenrheidiol sydd ei angen arnynt er mwyn iddynt weithredu.

  Mae hyn yn arbennig o berthnasol lle mae apiau'n gofyn am ganiatâd nad yw'n ymddangos ei fod yn gwneud synnwyr o ystyried natur yr ap. Er enghraifft, dylid bod yn amheus o ap Chwileiriausydd am gael mynediad at gysylltiadau defnyddiwr a gallu anfon negeseuon SMS. Dim ond cymwysiadau ag enw da wedi'i sefydlu o ffynonellau dibynadwy y dylid eu lawrlwytho a'u gosod.

- Ni ddylid cadw cyfrineiriau i borwyr gwe lleol. Mae hyn yn arbennig o bwysig lle mae mynediad a rennir i ddyfais neu borwr gwe. Eithriad i hyn yw pan ddefnyddir estyniad rheolwr cyfrinair diogel mewn porwr sydd angen ei ddatgloi (e.e. gyda chyfrinair arall) cyn y gellir adfer manylion y cyfrif sydd wedi'u cadw, fodd bynnag dylid cymryd gofal i sicrhau bod hwn wedi'i gloi/allgofnodi ar ôl ei ddefnyddio.

  Gall cadw manylion cyfrifon (enwau defnyddwyr / cyfrineiriau) ar borwyr gwe lleol y gall unrhyw un sy'n defnyddio'r porwr hwnnw eu cyrchu wedyn wanhau diogelwch cyfrif. Gall galluogi rheolaethau diogelwch ychwanegol ar gyfrifon fel 2SV/2FV/MFA neu ddefnyddio rheolwr cyfrinair diogel atal eraill rhag cael mynediad at gyfrifon mewn amgylchiadau o'r fath.

- Wrth ddefnyddio porwr a rennir, dylid clirio hanes a storfeydd porwr ar ôl eu defnyddio. Dylid ystyried defnyddio swyddogaethau pori preifat i leihau'r llwybr defnydd a adawir ar unrhyw borwr o'r fath hefyd.

Bod yn wyliadwrus bob math o ymdrechion peirianneg gymdeithasol /gwe-rwydo

- Dylid bod yn ofalus os derbynnir negeseuon e-bost, negeseuon sydyn, neu alwadau ffôn digymell neu annisgwyl yn gofyn am fanylion cyfrif neu wybodaeth bersonol neu gyfrinachol. Ni ddylid rhoi cyfrineiriau a chodau dilysu 2FA/MFA i unrhyw un.

  Bydd ymosodwyr yn aml yn ceisio 'hacio'r person' yn gyntaf gan ei fod yn rhatach ac yn gyflymach iddyn nhw nag ymosodiad technegol. Dylai staff canolfannau fod yn wyliadwrus o unrhyw un neu unrhyw beth sy'n ymddangos fel pe bai am ennill eu hymddiredaeth, eu rhuthro i wneud rhywbeth neu sy'n ymddangos yn rhyfedd. Os oes amheuaeth, rhowch y ffôn i lawr / peidiwch ag ymateb a pheidiwch â chlicio ar unrhyw gysylltau neu weithredu, a gwiriwch gyda pharti dibynadwy trwy sianel ddiogel (h.y. ffoniwch wasanaethau cwsmeriaid y corff dyfarnu trwy rif cymorth hysbys).

- Ni ddylai defnyddwyr fyth gymeradwyo na dilysu cais mewngofnodi na wnaethant ei ysgogi.

  Bydd ymosodwyr sy'n cael enw defnyddiwr a chyfrinair yn ceisio cael y defnyddiwr i rannu unrhyw god 2FA/MFA gyda nhw neu i gymeradwyo'r cais mewngofnodi trwy ryw fodd arall. Efallai y byddant yn ceisio argyhoeddi'r defnyddiwr bod angen iddo gadarnhau ei hunaniaeth a byddant yn anfon cod cyfrinachol y mae angen i'r defnyddiwr ei ddarllen wrthynt neu ofyn am gymeradwyaeth cais y maent yn ei anfon mewn ap dilysu. Mewn gwirionedd maent yn ceisio mewngofnodi i'r cyfrif, yn sbarduno 2FA/MFA ac yn ceisio twyllo'r defnyddiwr i roi'r cod hwnnw iddynt neu i gymeradwyo mynediad. Ni ddylid cymeradwyo ceisiadau i rannu codau / cymeradwyo mewngofnodi a dylid bod yn amheus iawn o geisiadau i wneud hynny.

- Peidiwch â chlicio ar gysylltau amheus, lawrlwytho atodiadau na sganio codau QR o ffynonellau anhysbys.

  Mae codau QR yn hawdd i ymosodwyr eu cynhyrchu ac yn cael eu defnyddio'n gynyddol mewn ymosodiadau gwe-rwydo. Mae angen bod yn ofalus wrth sganio cod QR a lle bynnag y bo modd, dylid defnyddio sganiwr cod QR diogel gydag enw da i helpu i fesur a yw cod QR yn amheus neu'n faleisus.

- Dylech wirio dilysrwydd unrhyw gyfathrebu trwy gysylltu a'r sefydliad yn uniongyrchol trwy sianeli swyddogol hysbys.

  Byddwch yn wyliadwrus o alwadau ffôn digymell i mewn hyd yn oed lle mae rhif y galwr yn ymddangos yn ddilys. Bydd ymosodwyr weithiau yn defnyddio gwasanaethau 'twyllo' ('spoofing') rhif sy'n cuddio eu rhif real ac yn gwneud iddo edrych fel bod yr alwad yn dod o rif dibynadwy gwirioneddol. Os oes amheuaeth, rhowch y ffôn i lawr a ffoniwch yn ôl ar rif y gellir ymddiried ynddo.

- Rhowch wybod am unrhyw ymdrechion gwe-rwydo sy'n cyfeirio at gyrff dyfarnu/eu systemau i'r corff dyfarnu dan sylw ar unwaith.

  Gall CGC a chyrff dyfarnu anfon cyfathrebiadau i ganolfannau lle gwelir ymosodiadau nodedig, ond maent yn dibynnu ar ganolfannau a staff canolfannau i dynnu eu sylw at ymosodiadau nodedig. Dylid rhoi gwybod i gyrff dyfarnu am unrhyw ymdrechion o'r fath.

Monitro cyfrifon ac adolygu mynediad cyfrifon yn rheolaidd

- Dylid adolygu cyfrifon staff y ganolfan fel mater o drefn ar gyfer unrhyw weithgaredd amheus, anarferol neu anawdurdodedig.

  Os gwelir unrhyw weithgarwch amheus, anarferol neu a allai fod heb awdurdod ar systemau cyrff dyfarnu, dylid rhoi gwybod i'r corff dyfarnu perthnasol ar unwaith, yn enwedig os credir y gallai diogelwch cyfrifon defnyddwyr fod wedi cael ei beryglu.

- Sicrhewch fod mynediad i ddefnyddwyr yn cael ei adolygu'n brydlon i staff sydd wedi gadael y ganolfan.

  Mae gadael mynediad cyn-weithiwr ar waith yn cynyddu'r perygl o fynediad amhriodol/anghyfreithlon i systemau a data.

- Dylech adolygu lefelau mynediad yn rheolaidd i sicrhau bod gan gyfrifon y lefel mynediad isaf o fynediad sydd ei angen ar gyfer eu rôl bresennol.

  Mae cyfrifon gorfreintiedig yn peri risg uwch pe bai ymosodwr yn cael mynediad i systemau'r ganolfan. Efallai ei bod yn ymddangos yn haws rhoi mynediad i staff i bopeth, ond os bydd ymosodwr yn mynd i mewn i gyfrif defnyddiwr, bydd ganddo fynediad at bopeth hefyd!

Arfer gorau seiberddiogelwch

Dylai canolfannau fod yn ymwybodol o'r bygythiadau a'r tueddiadau diogelwch diweddaraf mewn diogelwch cyfrifon ac addysgu staff ar sut i adnabod ymdrechion gwe-rwydo, diogelu dyfeisiau a diogelu systemau a data.

Mae'r Ganolfan Seiberddiogelwch Genedlaethol (NCSC) yn darparu cyngor seiberddiogelwch rhagorol a chynhwysfawr i ysgolion sydd yn berthnasol i bob canolfan – mae'r pwyntiau allweddol o hyn wedi'u cynnwys yn yr adran flaenorol.

Dylid dilyn cyngor a chanllawiau y Ganolfan Seiberddiogelwch Genedlaethol ar gyfer unrhyw systemau TG a ddefnyddir mewn canolfan, yn enwedig y rhai lle cedwir gwybodaeth am ddysgwyr, gwaith dysgwyr neu gofnodion asesu. Gall gwneud hynny atal effeithiau andwyol i staff a dysgwyr os bydd ymosodiad seiber.

Mae'r pynciau eraill a drafodir gan hyfforddiant Canolfan Seiberddiogelwch Genedlaethol yn cynnwys:

- Sefydlu polisi cyfrineiriau cadarn
- Galluogi dilysu aml-ffactor (MFA)
- Cadw meddalwedd a systemau yn gyfredol
- Gweithredu mesurau diogelwch rhwydwaith
- Cynnal copïau wrth gefn o ddata yn rheolaidd
- Addysgu gweithwyr ar ymwybyddiaeth o ddiogelwch
- Datblygu a phrofi cynllun ymateb i ddigwyddiadau
- Asesu ac archwilio rheolaethau diogelwch yn rheolaidd

Trwy fabwysiadu arferion gorau seiberddiogelwch safonol y diwydiant hyn, gall canolfannau leihau'r risg o ymosodiadau seiber yn sylweddol a diogelu eu data a'u hasedau gwerthfawr.

Os yw canolfannau'n cael profiad o ymosodiad seiber sy'n effeithio ar unrhyw ddata dysgwyr, cofnodion asesu neu waith dysgwyr, dylid cysylltu â'u corff dyfarnu ar unwaith i gael cyngor a chefnogaeth.