FG

Van:
Verzonden: dinsdag 24 november 2020 11:21
Aan:
Onderwerp: RE: [SURFcert#106753] Gelekte gebruikersnamen - wachtwoorden

Ho'

We zijn hiermee bezig.
Actieve accounts krijgen een mail om hun wachtwoord te wijzigen als het wachtwoord nog klopt dat er staat.

Een aantal accounts bestaat niet meer.

Grt

-----Oorspronkelijk bericht-----
Van: FG <fg@ou.nl>
Verzonden: dinsdag 24 november 2020 11:19
Aan: ; Privacyofficer <privacyofficer@ou.nl>
Onderwerp: RE: [SURFcert#106753] Gelekte gebruikersnamen - wachtwoorden

Dag allen,

Inmiddels is duidelijk om welke accounts het gaat. Graag onderzoeken of de wachtwoorden nog geldig zijn.
Indien deze nog geldig zijn, zullen deze collega's met spoed verzocht moeten worden het wachtwoord te wijzigen.

Een algemeen bericht naar alle medewerkers uit de lijst lijkt me op z'n plaats. Dit kan wat mij betreft via FG/PO óf ICT.
Hoe denken jullie hierover?

Zie ik iets over het hoofd?

Groeten,

-----Oorspronkelijk bericht-----
Van:
Verzonden: maandag 23 november 2020 21:46
Aan: ; FG <fg@ou.nl>; Privacyofficer <privacyofficer@ou.nl>
Onderwerp: FW: [SURFcert#106753] Gelekte gebruikersnamen - wachtwoorden

Hierover moeten een bericht maken en hoe te handelen denk ik.
Hebben we al eens eerder gedaan.
Ik stuur de FG en PO reeds een cc zodat dit samen verder opgepakt kan worden.

Grt

-----Oorspronkelijk bericht-----

Van: SURFcert - <cert@surfnet.nl>
Verzonden: maandag 23 november 2020 21:43
Aan: Cert <cert@ou.nl>
CC: SURFcert <cert@surfnet.nl>
Onderwerp: [SURFcert#106753] Gelekte gebruikersnamen - wachtwoorden

Beste CERT-OUNL,

== Waarom ontvangt u deze mail ==

Een online forum genaamd 'cit0day', dat gericht is op het verkopen van gestolen gebruikersnamen en wachtwoorden, heeft een inbraak gehad op zijn eigen database. Normaal gesproken moet er periodiek betaald worden om een update te krijgen van de wachtwoorden, nu liggen ze allemaal publiek op straat. Hierbij zitten ook accounts van Uw instelling. De inschatting is dat ongeveer 35% van de gebruikersnaam/wachtwoord combinaties nog niet in eerdere publicaties zijn geweest. Hieronder de link waarmee de wachtwoorden van Uw organisatie te downloaden zijn.

Er is niet meer info over waar de accounts oorspronkelijk gestolen zijn, of hoe lang dat geleden is.

== Downlad link ==

https://cernbox.cern.ch/index.php/s/8oj4a95JQudgGxs

== Wat verwacht SURFcert nu van jullie ==

Willen jullie van de betreffende accounts onderzoeken of de wachtwoorden nog geldig zijn en passende maatregelen nemen?
SURFcert zal het ticket sluiten, het hoeft niet afgemeld te worden.

== Openstaande incidenten ==

Hieronder staan eventueel de incidenten vermeld die op dit moment nog openstaan voor jullie instelling:
--

Met vriendelijke groeten,

SURFcert Officer on Duty
--
SURFcert . cert@SURFnet.nl . https://surf.nl/surfcert phone (24/7): GP: 0x4bc9be47bd783d33

Van:
Verzonden: dinsdag 24 november 2020 11:02
Aan:
Onderwerp: Via e-mail verzenden: 2020-11-24 [SURFcert#106753] Gelekte gebruikersnamen - wachtwoorden.docx
Bijlagen: 2020-11-24 [SURFcert#106753] Gelekte gebruikersnamen - wachtwoorden.docx

Hallo ,

Dit betreft een melding van SURFcert in verband met gehackte accounts van OU medewerkers die op een specifiek site staan die deze dan weer verkoopt. Deze site schijnt nu zelf ook gehackt te zijn waardoor de gehackte accounts op straat liggen. Deze lijst van OU medewerkers hebben wij van SURFcert ontvangen.

Grtz,

2020-11-24 [SURFcert#106753] Gelekte gebruikersnamen - wachtwoorden.docx

Marval #
SURFcert #
IP 145.20.xxx.

[SURFcert#106753] Gelekte gebruikersnamen - wachtwoorden

24-11-2020

Op 23-11 ontvingen we onderstaande mail van SURFcert:

Beste CERT-OUNL,

== Waarom ontvangt u deze mail ==

Een online forum genaamd 'cit0day', dat gericht is op het verkopen van gestolen gebruikersnamen en wachtwoorden, heeft een inbraak gehad op zijn eigen database. Normaal gesproken moet er periodiek betaald worden om een update te krijgen van de wachtwoorden, nu liggen ze allemaal publiek op straat. Hierbij zitten ook accounts van Uw instelling. De inschatting is dat ongeveer 35% van de gebruikersnaam/wachtwoord combinaties nog niet in eerdere publicaties zijn geweest. Hieronder de link waarmee de wachtwoorden van Uw organisatie te downloaden zijn.

Er is niet meer info over waar de accounts oorspronkelijk gestolen zijn, of hoe lang dat geleden is.

== Downlad link ==

https://cernbox.cern.ch/index.php/s/8oj4a95JQudgGxs

== Wat verwacht SURFcert nu van jullie ==

Willen jullie van de betreffende accounts onderzoeken of de wachtwoorden nog geldig zijn en passende maatregelen nemen?
SURFcert zal het ticket sluiten, het hoeft niet afgemeld te worden.

== Openstaande incidenten ==

Hieronder staan eventueel de incidenten vermeld die op dit moment nog openstaan voor jullie instelling:
--

Met vriendelijke groeten,
Remon Klein Tank
SURFcert Officer on Duty
--
SURFcert . cert@SURFnet.nl . https://surf.nl/surfcert phone (24/7): . PGP: 0x4bc9be47bd783d33

Onderstaand de lijst van de accounts die het betreft:

@OU.NL

Marval #
SURFcert #
IP 145.20.xxx.

@ou.nl
@ou.nl
@ou.nl:
@ou.nl
@ou.n
@ou.nl
@ou.nl
@ou.nl
@ou.nl
@ou.nl
@ou.nl
@ou.nl
@ou.nl:
@ou.nl:
@ou.nl
@ou.nl
@ou.nl:
@ou.nl
@ou.nl
@ou.nl
@ou.nl:
@ou.nl.
n@ou.nl
@ou.nl
@ou.nl
@ou.n
@ou.nl
@ou.nl
@ou.nl

\

Van:
Verzonden: dinsdag 24 november 2020 11:21
Aan:
Onderwerp: RE: Via e-mail verzenden: 2020-11-24 [SURFcert#106753] Gelekte gebruikersnamen - wachtwoorden.docx

Hallo

Die wachtwoorden kunnen wij uiteraard niet testen, maar vermoedelijk zijn dat oude wachtwoorden. Op de lijst staan ook medewerkers die niet meer bij de OU werken. Frontoffice gaat deze personen contacteren nu.

Grtz,

-----Oorspronkelijk bericht-----
Van: \
Verzonden: dinsdag 24 november 2020 11:12
Aan:
Onderwerp: RE: Via e-mail verzenden: 2020-11-24 [SURFcert#106753] Gelekte gebruikersnamen - wachtwoorden.docx

Hoi

Kunnen jullie nagaan of van de betreffende accounts de wachtwoorden nog geldig zijn? Indien deze nog geldig zijn, moeten we deze collega's met spoed verzoeken het e-mailadres aan te passen.

Zie ik nog iets over het hoofd?

Groeten.

-----Oorspronkelijk bericht-----
Van:
Verzonden: dinsdag 24 november 2020 11:02
Aan:
Onderwerp: Via e-mail verzenden: 2020-11-24 [SURFcert#106753] Gelekte gebruikersnamen - wachtwoorden.docx

Hallo

Dit betreft een melding van SURFcert in verband met gehackte accounts van OU medewerkers die op een specifiek site staan die deze dan weer verkoopt. Deze site schijnt nu zelf ook gehackt te zijn waardoor de gehackte accounts op straat liggen. Deze lijst van OU medewerkers hebben wij van SURFcert ontvangen.

Grtz,

2020-11-24 [SURFcert#106753] Gelekte gebruikersnamen - wachtwoorden.docx

FG

Van:
Verzonden: dinsdag 24 november 2020 12:48
Aan: FG; ; Privacyofficer;
CC:
Onderwerp: Re: [SURFcert#106753] Gelekte gebruikersnamen - wachtwoorden

Dag

Weet dat in 95% van de gevallen dit veroorzaakt wordt door hergebruik van wachtwoorden (en gebruikersnamen) bij diensten buiten de OU. Of te wel onderstaande zegt niks over hoe/waar de gegevens dan zijn ontvreemd.
Ik weet dat bij de grote linkedIN hack een aantal jaar geleden, veel ou accounts in dat soort lijsten terecht zijn gekomen (waaronder mijn eigen).

Of dat hier het geval is kan ik niet beoordelen, maar we kunnen ook niet zomaar aannemen dat ze bij de OU zelf zijn ontvreemd of dat het überhaupt ooit geldige wachtwoorden bij de OU zijn geweest. Als ik naar de lijst kijk twijfel ik daar zelfs over omdat er wachtwoorden bij zitten die niet aan de OU ww policy voldoen. In mijn geval was het wachtwoord dat destijds bij @ou.nl stond niet mijn OU wachtwoord, maar mijn LinkedIN wachtwoord. Of te wel het OU account is nooit in gevaar geweest.

Onderzoek zou hier duidelijkheid in kunnen geven...maar dat is makkelijker gezegd dan gedaan. Zijn er indicaties voor misbruik op dit moment?

Groeten

On 24/11/2020, 12:37, "FG" <fg@ou.nl> wrote:

Dag

Ik lees dat 'cit0day' een inbraak heeft gehad in de eigen database. Ik vraag me af hoe 'cit0day' überhaupt aan de gebruikersnamen en wachtwoorden komt. Het gaat al om gestolen wachtwoorden.

Met betrekking tot het datalek, kan het wellicht zo zijn het nu om oude wachtwoorden gaat. Wel is het zo dat het op enig moment wél een actueel wachtwoord betrof. Ik lees dat de inschatting is dat ongeveer 35% van de gebruikersnaam/wachtwoord combinaties nog niet in eerdere publicaties zijn geweest.

Volgens mij kunnen we niet uitsluiten dat de wachtwoorden (toen deze wel actueel waren) en mailadressen via cit0day eerder werden verkocht en dus konden worden misbruikt. Het feit dat mailadressen en wachtwoorden op straat lagen is natuurlijk een kwalijke zaak, ongeacht of deze wel/niet actueel zijn. Op de een of andere manier is het partijen gelukt om toegang te krijgen tot de wachtwoorden.
Mocht deze denkwijze niet correct zijn, hoor ik het graag.

Met vriendelijke groet,

| functionaris gegevensbescherming

Werkdagen: maandag, dinsdag, woensdag en donderdag

Human resources, juridische zaken en inkoop | Juridische Zaken
bezoekadres: Valkenburgerweg 177 Heerlen | ATH 2.22
postadres: Postbus 2960 6401 DL Heerlen
| E FG@ou.nl

FG

Van:
Verzonden: dinsdag 24 november 2020 14:14
Aan: : FG;); Privacyofficer; .k
CC:
Onderwerp: Re: [SURFcert#106753] Gelekte gebruikersnamen - wachtwoorden

Er staan @ou mailadressen en wachtwoorden... laten we eerst een valideren dat het OU-accounts betreft (zie ook mijn vorige mail).

On 24/11/2020, 14:11, "J

Allen,

Ik zou dit als een data lek kwalificeren, dat een aantal accounts niet meer actief zijn of dat de wachtwoorden inmiddels zijn veranderd is niet relevant; deze condities reduceren alleen de impact van dit incident.
Ik lees in de CERN communicatie allen dat cit0day zelf is gehackt waardoor hun inhoud openbaar werd, ik lees geen enkele indicatie hoe de OU accounts en wachtwoord in deze omgeving zijn gekomen, correct?

-----Oorspronkelijk bericht-----
Van: J >
Verzonden: dinsdag 24 november 2020 12:25
Aan: FG <fg@ou.nl>; ! >; Privacyofficer <privacyofficer@ou.nl>;
P
CC:

Onderwerp: RE: [SURFcert#106753] Gelekte gebruikersnamen - wachtwoorden

Hoi

Volgens mij staat in het bericht van CERT hoe dit veroorzaakt is.

Dan vwb datalek:
Bij de communicatie naar de afzonderlijke medewerkers kunnen we tevens vragen of het wachtwoord nog klopte. Wij vermoeden nl dat dit oude wachtwoorden zijn.
Is het bij ieder actief account een oud wachtwoord dan is het m.i. geen datalek.

Grt

-----Oorspronkelijk bericht-----
Van: FG <fg@ou.nl>
Verzonden: dinsdag 24 november 2020 11:53
Aan: J
<privacyofficer@ou.nl>:

Onderwerp: RE: [SURFcert#106753] Gelekte gebruikersnamen - wachtwoorden

Dag collega's,

Ik heb een aantal collega's in de CC toegevoegd om iedereen aangesloten te houden.

We moeten concluderen dat op enig moment van (snel geteld) 31 medewerkers inlognaam en wachtwoord van de OU account bekend waren en dat deze beschikbaar werden gesteld via online forum genaamd 'cit0day'. Volgens mij kunnen we misbruik niet uitsluiten en zie ik geen andere mogelijkheid dan dit incident aan te merken als een datalek.

Ik zou jullie in ieder geval willen vragen te onderzoeken hoe het mogelijk is dat deze wachtwoorden bekend zijn voor 'de buitenwereld'.

Voorheen deelde ik mijn standpunt met ' ĸ, alvorens samen het Cvb te informeren. Ik stel voor dat ik dit maal mijn standpunt deel met alvorens samen het Cvb te informeren.

Indien jullie een andere mening hebben, hoor ik dit graag.

Met vriendelijke groet,

¦ functionaris gegevensbescherming

Werkdagen: maandag, dinsdag, woensdag en donderdag

Human resources, juridische zaken en inkoop | Juridische Zaken
bezoekadres: Valkenburgerweg 177 Heerlen | ATH 2.22
postadres: Postbus 2960 6401 DL Heerlen
| E FG@ou.nl

-----Oorspronkelijk bericht-----
Van: nl>
Verzonden: dinsdag 24 november 2020 11:21
Aan: FG <fg@ou.nl>; ';>; Privacyofficer
Onderwerp: RE: [SURFcert#106753] Gelekte gebruikersnamen - wachtwoorden

Hoi

We zijn hiermee bezig.
Actieve accounts krijgen een mail om hun wachtwoord te wijzigen als het wachtwoord nog klopt dat er staat.

Een aantal accounts bestaat niet meer.

Grt

-----Oorspronkelijk bericht-----
Van: FG <fg@ou.nl>
Verzonden: dinsdag 24 november 2020 11:19
Aan:
<privacyofficer@ou.nl>
Onderwerp: RE: [SURFcert#106753] Gelekte gebruikersnamen - wachtwoorden

Dag allen,

Inmiddels is duidelijk om welke accounts het gaat. Graag onderzoeken of de wachtwoorden nog geldig zijn.
Indien deze nog geldig zijn, zullen deze collega's met spoed verzocht moeten worden het wachtwoord te wijzigen.

Een algemeen bericht naar alle medewerkers uit de lijst lijkt me op z'n plaats. Dit kan wat mij betreft via FG/PO óf ICT.
Hoe denken jullie hierover?

Zie ik iets over het hoofd?

Groeten,

-----Oorspronkelijk bericht-----
Van: J
Verzonden: maandag 23 november 2020 21:46
Aan: I , . G <fg@ou.nl>; Privacyofficer <privacyofficer@ou.nl>
Onderwerp: FW: [SURFcert#106753] Gelekte gebruikersnamen - wachtwoorden

Hierover moeten een bericht maken en hoe te handelen denk ik.
Hebben we al eens eerder gedaan.
Ik stuur de FG en PO reeds een cc zodat dit samen verder opgepakt kan worden.

Grt

-----Oorspronkelijk bericht-----
Van: SURFcert · cert@surfnet.nl>
Verzonden: maandag 23 november 2020 21:43
Aan: Cert <cert@ou.nl>
CC: SURFcert <cert@surfnet.nl>
Onderwerp: [SURFcert#106753] Gelekte gebruikersnamen - wachtwoorden

Beste CERT-OUNL,

== Waarom ontvangt u deze mail ==

Een online forum genaamd 'cit0day', dat gericht is op het verkopen van gestolen gebruikersnamen en wachtwoorden, heeft een inbraak gehad op zijn eigen database. Normaal gesproken moet er periodiek betaald worden om een update te krijgen van de wachtwoorden, nu liggen ze allemaal publiek op straat. Hierbij zitten ook accounts van Uw instelling. De inschatting is dat ongeveer 35% van de gebruikersnaam/wachtwoord combinaties nog niet in eerdere publicaties zijn geweest. Hieronder de link waarmee de wachtwoorden van Uw organisatie te downloaden zijn.

Er is niet meer info over waar de accounts oorspronkelijk gestolen zijn, of hoe lang dat geleden is.

== Downlad link ==

https://cernbox.cern.ch/index.php/s/8oj4a95JQudgGxs

== Wat verwacht SURFcert nu van jullie ==

Willen jullie van de betreffende accounts onderzoeken of de wachtwoorden nog geldig zijn en passende maatregelen nemen?
SURFcert zal het ticket sluiten, het hoeft niet afgemeld te worden.

== Openstaande incidenten ==

Hieronder staan eventueel de incidenten vermeld die op dit moment nog openstaan voor jullie instelling:
--

Met vriendelijke groeten,

SURFcert Officer on Duty
--
SURFcert . cert@SURFnet.nl . https://surf.nl/surfcert phone (24/7) [illegible]o4 . PGP: 0x4bc9be47bd783d33

FG

Van: FG
Verzonden: dinsdag 24 november 2020 12:53
Aan:
CC:
Onderwerp: RE: [SURFcert#106753] Gelekte gebruikersnamen - wachtwoorden

Dag

Morgen zal ik mijn standpunt met jou delen, in ieder geval dat er sprake is van een datalek (met mogelijk een aantal overwegingen). Hierover kunnen we een gesprek voeren en afhankelijk van de uitkomst, stappen we morgen samen naar het Cvb. Het informeren van het Cvb doe ik het liefst ook morgen (i.v.m. de termijn van 72 uur).

Met vriendelijke groet,

unctionaris gegevensbescherming

Werkdagen: maandag, dinsdag, woensdag en donderdag

Human resources, juridische zaken en inkoop | Juridische Zaken
bezoekadres: Valkenburgerweg 177 Heerlen | ATH 2.22
postadres: Postbus 2960 6401 DL Heerlen
T | E FG@ou.nl

Open Universiteit

Van:
Verzonden: dinsdag 24 november 2020 12:46
Aan: FG <fg@ou.nl>; >
CC:
Onderwerp: RE: [SURFcert#106753] Gelekte gebruikersnamen - wachtwoorden

Beste collega's, ik probeer in sneltrein vaart bij te lezen, is er op dit moment een escalatie nodig of zitten we in de analyse van de gelekte data?

Met vriendelijke groet

Van: FG <fg@ou.nl>
Verzonden: dinsdag 24 november 2020 12:44

Aan:
CC:
Onderwerp: RE: [SURFcert#106753] Gelekte gebruikersnamen - wachtwoorden

Hoi

Klopt! Ik besprak het vanmorgen ook al met deze zal ik aanpassen.

Groetjes,

Van:
Verzonden: dinsdag 24 november 2020 12:43
Aan: FG <fg@ou.nl>
CC:
Onderwerp: RE: [SURFcert#106753] Gelekte gebruikersnamen - wachtwoorden

Trouwens, even iets anders. Ergens las ik iets over
M.i. moet de procedure van datalekken aangepast worden.
als directeur moet de rol van escalatie hebben.
Pas jij die aan of zullen wij dat doen?

Van: FG <fg@ou.nl>
Verzonden: dinsdag 24 november 2020 12:38
Aan:
CC: ; Privacyofficer <privacyofficer@ou.nl>;

Onderwerp: RE: [SURFcert#106753] Gelekte gebruikersnamen - wachtwoorden

Mooi!

Van:
Verzonden: dinsdag 24 november 2020 12:35
Aan: FG <fg@ou.nl>
CC: >; Privacyofficer <privacyofficer@ou.nl>;

Onderwerp: FW: [SURFcert#106753] Gelekte gebruikersnamen - wachtwoorden

Dag

Reeds ter info.
Verder updates volgen dan.
Zoals je ziet veel accounts die niet meer gebruikt worden.

Grt

Van:
Verzonden: dinsdag 24 november 2020 12:31
Aan:
CC:
Onderwerp: RE: [SURFcert#106753] Gelekte gebruikersnamen - wachtwoorden

Hoi

Ter info; iedereen is gecontacteerd.
De meeste heb ik via Teams benaderd, ik wacht nu op respons.
Bijgevoegd een Excelblad met de lijst van personen, contactwijze en respons die gegeven is.
Ik zal dit in de gaten houden en eventueel medewerkers opnieuw benaderen die geen respons geven.

Met vriendelijke groet,

Informatietechnologie en facilitaire zaken | Operations
bezoekadres: Valkenburgerweg 177 Heerlen
postadres: Postbus 2960 6401 DL Heerlen

Open Universiteit
www.ou.nl

Van:
Verzonden: dinsdag 24 november 2020 11:29
Aan:
Onderwerp: FW: [SURFcert#106753] Gelekte gebruikersnamen - wachtwoorden
Urgentie: Hoog

Ter info; graag niet reageren op deze mail richting de betrokkenen...
Bedoeling is dus mail sturen naar betrokkenen (controleren of er geen accounts bij zijn die misschien al niet meer actief zijn c.q. niet meer bestaan).
Tekstvoorbeeld staat in de call.
Wachtwoord wat in de lijst staat moet dus mee worden gecommuniceerd in de mail (zie hieronder in geel).

Grt,

-----Oorspronkelijk bericht-----
Van:
Verzonden: dinsdag 24 november 2020 11:21
Aan: FG <fg@ou.nl>; il>; Privacyofficer <privacyofficer@ou.nl>;

Onderwerp: RE: [SURFcert#106753] Gelekte gebruikersnamen - wachtwoorden

Hoi

We zijn hiermee bezig.
Actieve accounts krijgen een mail om hun wachtwoord te wijzigen als het wachtwoord nog klopt dat er staat.

Een aantal accounts bestaat niet meer.

Grt

-----Oorspronkelijk bericht-----
Van: FG <fg@ou.nl>
Verzonden: dinsdag 24 november 2020 11:19
Aan:
<privacyofficer@ou.nl>
Onderwerp: RE: [SURFcert#106753] Gelekte gebruikersnamen - wachtwoorden

Dag allen,

Inmiddels is duidelijk om welke accounts het gaat. Graag onderzoeken of de wachtwoorden nog geldig zijn.
Indien deze nog geldig zijn, zullen deze collega's met spoed verzocht moeten worden het wachtwoord te wijzigen.

Een algemeen bericht naar alle medewerkers uit de lijst lijkt me op z'n plaats. Dit kan wat mij betreft via FG/PO óf ICT.
Hoe denken jullie hierover?

Zie ik iets over het hoofd?

Groeten,

-----Oorspronkelijk bericht-----
Van:
Verzonden: maandag 23 november 2020 21:46
Aan: >; FG <fg@ou.nl>; Privacyofficer <privacyofficer@ou.nl>
Onderwerp: FW: [SURFcert#106753] Gelekte gebruikersnamen - wachtwoorden

Hierover moeten een bericht maken en hoe te handelen denk ik.
Hebben we al eens eerder gedaan.
Ik stuur de FG en PO reeds een cc zodat dit samen verder opgepakt kan worden.

Grt

-----Oorspronkelijk bericht-----
Van: SURFcert - <cert@surfnet.nl>
Verzonden: maandag 23 november 2020 21:43
Aan: Cert <cert@ou.nl>
CC: SURFcert <cert@surfnet.nl>
Onderwerp: [SURFcert#106753] Gelekte gebruikersnamen - wachtwoorden

Beste CERT-OUNL,

== Waarom ontvangt u deze mail ==

Een online forum genaamd 'cit0day', dat gericht is op het verkopen van gestolen gebruikersnamen en wachtwoorden, heeft een inbraak gehad op zijn eigen database. Normaal gesproken moet er periodiek betaald worden om een update te krijgen van de wachtwoorden, nu liggen ze allemaal publiek op straat. Hierbij zitten ook accounts van Uw instelling. De inschatting is dat ongeveer 35% van de gebruikersnaam/wachtwoord combinaties nog niet in eerdere publicaties zijn geweest. Hieronder de link waarmee de wachtwoorden van Uw organisatie te downloaden zijn.

Er is niet meer info over waar de accounts oorspronkelijk gestolen zijn, of hoe lang dat geleden is.

== Downlad link ==

https://cernbox.cern.ch/index.php/s/8oj4a95JQudgGxs

== Wat verwacht SURFcert nu van jullie ==

Willen jullie van de betreffende accounts onderzoeken of de wachtwoorden nog geldig zijn en passende maatregelen nemen?
SURFcert zal het ticket sluiten, het hoeft niet afgemeld te worden.

== Openstaande incidenten ==

Hieronder staan eventueel de incidenten vermeld die op dit moment nog openstaan voor jullie instelling:
--

Met vriendelijke groeten,

SURFcert Officer on Duty
--
SURFcert . cert@SURFnet.nl . https://surf.nl/surfcert phone (24/7): [redacted] . PGP: 0x4bc9be47bd783d33

FG

Van:
Verzonden: dinsdag 13 april 2021 21:20
Aan: FG
CC:
Onderwerp: Oud incident uit 2020: toen wel of niet behandeld (en gemeld) als datalek?

Hi

De verdachte inlog van collega vorig jaar december ontbrak op mijn incidentenrapportage. Was het behandeld als datalek en heb jij er een verslagje van dat ik aan de CERT rapportage kan toevoegen? In Marval kan ik er juist geen call van vinden, mogelijk omdat de Servicedesk er niet bij betrokken is geraakt.

Dank je en groet,

| Chief Information Security & Quality Officer

Informatietechnologie en facilitaire zaken | Innovatie en development
bezoekadres: Valkenburgerweg 177 Heerlen
postadres: Postbus 2960 6401 DL Heerlen

Open Universiteit
www.ou.nl

Van:
Verzonden: vrijdag 27 november 2020 09:30
Aan:

Onderwerp: RE: contact ivm melden datalek?

We gaan melden aan de AP.

Is onderstaande inlog op te volgen?

Van:
Verzonden: vrijdag 27 november 2020 09:13
Aan:

Onderwerp: Re: contact ivm melden datalek?

Heb nog even in onze MS Advanced Threat protectie logs gekeken voor alle users vanaf regel 14. Van deze users zijn 2 meldingen, waarvan 1 zorgelijk:
Atypical travel bij (maar dat kan ook VPN zijn, of device thuis terwijl op vakantie etc)

User's risk report | User's sign-ins | User's risky sign-ins | Linked risky sign-in

Detection type	Atypical travel	Activity	Sign-in
Risk state	At risk	Detection time	9/5/202(
Risk level	Medium	Detection last updated	9/5/202(
Risk detail	-	Token issuer type	Azure Al
Source	Identity Protection	Travel duration	4:43
Detection timing	Offline		

En niet Atypical, maar nieuwe locaties, normaal gesproken niks mee aan de hand)

9/7/2020, 10:40:15 AM	145.20.80.4	Amst
9/1/2020, 9:38:15 AM	185.61.72.122	Bruss

Beide users zijn inmiddels ook al met 2FA uitgerold dus zouden nu ook de 2FA verplichting krijgen bij zo'n login.
heeft 2FA sinds 3-11, sinds 19-8

From:
Date: Friday, 27 November 2020 at 08:45
To:

Subject: FW: contact ivm melden datalek?

FYI, we gaan een overleg in met de CvB

Van: FG <fg@ou.nl>
Verzonden: vrijdag 27 november 2020 08:35
Aan:
Onderwerp: contact ivm melden datalek?

Dag

Ik sta nog steeds achter het melden van dit datalek, nu we een deel niet kunnen uitsluiten. De AP voert een vrij strikt beleid ten aanzien van het melden van dit soort zaken. Wel hebben we natuurlijk een sterk verhaal!
Wanneer zie jij tijd deze ochtend om samen het Cvb te contacteren? Mocht het niet mogelijk zijn om samen te gaan, dan kan ik (na eventuele afstemming) zelf naar het Cvb stappen.

Met vriendelijke groet,

| functionaris gegevensbescherming

Werkdagen: maandag, dinsdag, woensdag en donderdag

Human resources, juridische zaken en inkoop | Juridische Zaken
bezoekadres: Valkenburgerweg 177 Heerlen | ATH 2.22
postadres: Postbus 2960 6401 DL Heerlen
E FG@ou.nl

Open Universiteit

FG

Van:
Verzonden: woensdag 25 november 2020 11:04
Aan: FG;
CC: Privacyofficer
Onderwerp: RE:

Hi edankt,

Zojuist met gesproken we wachten nog even de resultaten af van dit onderzoek. De kernvraag is inderdaad:

- Is de combinatie userid /wachtwoord gebruikt geweest voor een OU, applicatie of service (neem hier ook Surf in mee)? Zo ja, welke periode

We hebben 72 uur vanaf 24 nov, 12:00 uur, ik stel voor dat we de personen direct benaderen met deze vraag en dat we het onderzoek de tijd geven tot 26-11 eind van de middag.

Daarnaast lijken er 3 of 4 wachtwoorden gegenereerd te zijn, is er na te gaan of een van de OU services deze kan genereren?

Met vriendelijke groet

Van:
Verzonden: woensdag 25 november 2020 10:34
Aan: FG <fg@ou.nl>;
CC: Privacyofficer <privacyofficer@ou.nl>
Onderwerp: FW:

FYI een update van de statussen.

Tevens laat ik nog specifiek navragen of het wachtwoord wel klopte bij personen die nu aangeven dat ze het wachtwoord gewijzigd hebben.
Bovendien laat ik navragen of dat dan het wachtwoord was voor inloggen bij de OU, of bijv social media/LinkedIn etc.

Wordt vervolgd

Grt

Medewerkers		Opmerking
		Teams bericht verzonden
	2907a	Gemaild
		Teams bericht verzonden
		Teams bericht verzonden
		Teams bericht verzonden
		Teams bericht verzonden
		Teams bericht verzonden
		Teams bericht verzonden
		Teams bericht verzonden
	l06e101	Gemaild
		Teams bericht verzonden
		Teams bericht verzonden
		Teams bericht verzonden
		Teams bericht verzonden
	93106	Teams bericht verzonden
		Gemaild

Respons

Wachtwoord is aangepast
Wachtwoord klopt niet
Wachtwoord klopt niet

Wachtwoord klopt niet
Wachtwoord is aangepast
Wachtwoord wordt al 5 jaar niet meer gebruikt

Wachtwoord klopt niet
Wachtwoord klopt niet
Wachtwoord klopt niet

FG

Van: J
Verzonden: woensdag 25 november 2020 11:19
Aan: FG;
CC: Privacyofficer;
Onderwerp: RE:

Hallo allen,

Al jullie vragen zijn gesteld aan de gebruikers.
Er komt een update.
Niet iedereen is te bereiken helaas, niet via mail (geen antwoord), niet via Teams. Staat er op de profieldienst geen 06-nr en is OU-nr niet doorgeschakeld dan wordt het moeilijk.

vraagt of wachtwoorden vanuit OU-systemen gegenereerd kunnen zijn. Dat is toch niet het geval?

Grt

Van: FG <fg@ou.nl>
Verzonden: woensdag 25 november 2020 11:07
Aan:
CC: Privacyofficer <privacyofficer@ou.nl>
Onderwerp: RE:

Dag

Mogelijk een onzinnige vraag, maar mag ik aannemen dat de medewerkers die aangeven 'wachtwoord klopt niet' bedoelen dat zij met zekerheid kunnen zeggen dat zij dit wachtwoord nooit hebben gebruikt voor de OU account? Ik weet niet welk bericht de medewerkers hebben ontvangen, waardoor de reactie 'klopt niet' voor mij te vaag is.

Met vriendelijke groet,

unctionaris gegevensbescherming

Werkdagen: maandag, dinsdag, woensdag en donderdag

Human resources, juridische zaken en inkoop | Juridische Zaken
bezoekadres: Valkenburgerweg 177 Heerlen | ATH 2.22
postadres: Postbus 2960 6401 DL Heerlen
| E E FG@ou.nl

Open Universiteit

Van: Janssen, Hilde <
Verzonden: woensdag 25 november 2020 10:34
Aan: FG <fg@ou.nl>: R
CC: Privacyofficer <privacyofficer@ou.nl>
Onderwerp: FW:

FYI een update van de statussen.

Tevens laat ik nog specifiek navragen of het wachtwoord wel klopte bij personen die nu aangeven dat ze het wachtwoord gewijzigd hebben.
Bovendien laat ik navragen of dat dan het wachtwoord was voor inloggen bij de OU, of bijv social media/LinkedIn etc.

Wordt vervolgd

Grt

FG

Van:
Verzonden: woensdag 25 november 2020 11:21
Aan: FG; J
CC: : Privacyofficer
Onderwerp: Functies medewerkers CERN melding

Allen,

Focus op risico voor persoonsgegevens is uiteraard belangrijk. Daarnaast is het mogelijk dat er (in mailboxen vooral) bedrijfsgegevens te vinden zijn. Is nog redelijkerwijs te achterhalen welke functies deze personen hadden – en wat zou het traject voor zijn? Indien het tevens onderzoekers betreft, zou het kunnen gaan om afgetapte onderzoeksgegevens.
Het zou naar mijn inschatting wel "bijvangst" van wachtwoorddieven zijn. Gerichte aanval zit er zelden achter, het gaat vaak om wachtwoorden om spam te kunnen versturen vanuit een bestaande mailbox.

Groet,

(Chief Information) Security Officer

Van: FG <fg@ou.nl>
Verzonden: woensdag 25 november 2020 11:07
Aan:
CC:
Onderwerp: RE:

Dag I

Mogelijk een onzinnige vraag, maar mag ik aannemen dat de medewerkers die aangeven 'wachtwoord klopt niet' bedoelen dat zij met zekerheid kunnen zeggen dat zij dit wachtwoord nooit hebben gebruikt voor de OU account? Ik weet niet welk bericht de medewerkers hebben ontvangen, waardoor de reactie 'klopt niet' voor mij te vaag is.

Met vriendelijke groet,

| functionaris gegevensbescherming

Werkdagen: maandag, dinsdag, woensdag en donderdag

Human resources, juridische zaken en inkoop | Juridische Zaken
bezoekadres: Valkenburgerweg 177 Heerlen | ATH 2.22
postadres: Postbus 2960 6401 DL Heerlen
| E FG@ou.nl

Open Universiteit

FG

Van:
Verzonden: woensdag 25 november 2020 11:33
Aan: FG; I ; Privacyofficer; I
Onderwerp: FW:
Bijlagen: CERT Wachtwoorden.xlsx

FYI, de status op dit moment met antwoorden.

Van:
Verzonden: woensdag 25 november 2020 11:29
Aan:
Onderwerp: RE:

Hoi

Zie hier het volledig bijgewerkte overzicht.

Met vriendelijke groet,

Informatietechnologie en facilitaire zaken | Operations
bezoekadres: Valkenburgerweg 177 Heerlen
postadres: Postbus 2960 6401 DL Heerlen
T 045

Open Universiteit
www.ou.nl

Van:
Verzonden: woensdag 25 november 2020 10:32
Aan: I
Onderwerp: RE:

Hoi

Bedankt, kun je svp toch nog eens doorvragen bij de mensen die aangeven, wachtwoord is aangepast of het wachtwoord klopte en of men daar nog mee werkte en of dit voor de OU was of bijv voor LinkedIn.
Dat is van belang om te weten.

Grt

Van:
Verzonden: woensdag 25 november 2020 08:52
Aan:
Onderwerp: RE:

Hoi

Ik wacht nog op een aantal antwoorden van medewerkers.
Ik heb de medewerkers niet specifiek gevraagd of het wachtwoord herkent wordt.
Tot nu toe hebben de medewerkers die getroffen zijn aangegeven dat het wachtwoord helemaal niet bekend is of ooit gebruikt is.

Met vriendelijke groet,

Informatietechnologie en facilitaire zaken | Operations
bezoekadres: Valkenburgerweg 177 Heerlen
postadres: Postbus 2960 6401 DL Heerlen
T 045 - 576

Open Universiteit
www.ou.nl

Van:
Verzonden: dinsdag 24 november 2020 23:22
Aan:
Onderwerp:

Heb je al een bijgewerkt document vwb de gelekte wachtwoorden?

Heb je de medewerkers ook gevraagd of het wachtwoord inderdaad gebruikt wordt en of dit voor andere zaken is dan de OU.
Bijv voor LinkedIn?

Grt

Open Universiteit
www.ou.nl

Dienst Informatietechnologie en facilitaire zaken
bezoekadres: Valkenburgerweg 177 Heerlen
postadres: Postbus 2960 6401 DL Heerlen

Medewerkers		Opmerking
		Teams bericht verzonden
	2907a	Gemaild
		Teams bericht verzonden
		Teams bericht verzonden
		Teams bericht verzonden
		Teams bericht verzonden
		Teams bericht verzonden
		Teams bericht verzonden
		Teams bericht verzonden
	06e101	Gemaild
		Teams bericht verzonden
		Teams bericht verzonden
		Teams bericht verzonden
		Teams bericht verzonden
	3106	Teams bericht verzonden
		Gemaild

Respons
Wachtwoord klopt niet
Wachtwoord is aangepast
Wachtwoord klopt niet
Wachtwoord klopt niet
Wachtwoord klopt niet
Wachtwoord klopt niet
Wachtwoord is aangepast
Wachtwoord wordt al 5 jaar niet meer gebruikt
Wachtwoord klopt niet
Wachtwoord klopt niet
Wachtwoord klopt niet
Wachtwoord klopt niet
Wachtwoord klopt niet

Wachtwoord ooit eerder gebruikt of bij andere websites?
Gebruikte het wachtwoord vele-jaar geleden (Kan geen tijdsbestek aangeven). Gebruikte het wachtwoord en veranderd het cijfer ieder jaar. Vanaf maart/april dit jaa
Voor de zekerheid het wachtwoord gewijzigd (had het wachtwoord nog nooit gebruikt)
Nee, wachtwoord nog nooit gebruikt.
Nee, wachtwoord nog nooit gebruikt.
Nee, wachtwoord nog nooit gebruikt.
Geen antwoord via mail, niet via Teams bereikbaar. Telefoonnummer onbekend
Nee, wachtwoord nog nooit gebruikt.
Voor de zekerheid het wachtwoord gewijzigd (had het wachtwoord nog nooit gebruikt)
Wachtwoord wordt al 5 jaar niet meer gebruikt
Geen antwoord via mail, niet via Teams bereikbaar. Telefoonumme 5 werd niet opgenomen.
Nee, wachtwoord nog nooit gebruikt.
Nee, wachtwoord nog nooit gebruikt.
Nee, wachtwoord nog nooit gebruikt.
Nee, wachtwoord nog nooit gebruikt.
Nee, wachtwoord nog nooit gebruikt.
Geen antwoord via mail, niet via Teams bereikbaar. Telefoonnummer onbekend

ır komt het wachtwoord niet meer voor bij zijn OU-account. Heeft het wachtwoord mogelijk ook bij zijn ıruikt. Dit kan c

lie niet met zekerheid zeggen

FG

Van:
Verzonden: woensdag 25 november 2020 13:35
Aan: FG;
CC: ., Privacyofficer;
Onderwerp: Re:

Opvolgingsvlag: Opvolgen
Vlagstatus: Met vlag

Tja...er is vooralsnog geen aanleiding om hier vanuit te gaan. Dan was de lijst denk ik ook langer geweest.
Onze IAM omgeving is onderdeel van de jaarlijkse digid audit (incl pentest), maar dat is natuurlijk ook nog geen garantie. Er zijn in ieder geval geen afwijkingen gezien in (audit) logs etc.
Ook een aantal wachtwoorden voldoen niet aan onze password policy en bij ons log je als medewerker niet in met je mailadres.

De interviews geven hopelijk meer inzicht...en wellicht zien we op basis van de lijst medewerkers een samenhang (rol of afdeling of gebruik van ww in specifieke applicatie of iets dergelijks)?

Groeten

From:
Date: Wednesday, 25 November 2020 at 11:19
To: FG <fg@ou.nl>,
Cc: " ıl>, Privacyofficer <privacyofficer@ou.nl>

Subject: RE:

Hallo allen,

Al jullie vragen zijn gesteld aan de gebruikers.
Er komt een update.
Niet iedereen is te bereiken helaas, niet via mail (geen antwoord), niet via Teams. Staat er op de profieldienst geen 06-nr en is OU-nr niet doorgeschakeld dan wordt het moeilijk.

agt of wachtwoorden vanuit OU-systemen gegenereerd kunnen zijn. Dat is toch niet het geval?

Grt

Van: FG <fg@ou.nl>
Verzonden: woensdag 25 november 2020 11:07
Aan:
CC: rivacyofficer <privacyofficer@ou.nl>
Onderwerp: RE:

Dag

Mogelijk een onzinnige vraag, maar mag ik aannemen dat de medewerkers die aangeven 'wachtwoord klopt niet' bedoelen dat zij met zekerheid kunnen zeggen dat zij dit wachtwoord nooit hebben gebruikt voor de OU account? Ik weet niet welk bericht de medewerkers hebben ontvangen, waardoor de reactie 'klopt niet' voor mij te vaag is.

Met vriendelijke groet,

·n | functionaris gegevensbescherming

Werkdagen: maandag, dinsdag, woensdag en donderdag

Human resources, juridische zaken en inkoop | Juridische Zaken
bezoekadres: Valkenburgerweg 177 Heerlen | ATH 2.22
postadres: Postbus 2960 6401 DL Heerlen
T | **E** FG@ou.nl

Open Universiteit

Van:
Verzonden: woensdag 25 november 2020 10:34
Aan: FG <fg@ou.nl>;
CC: Privacyofficer <privacyofficer@ou.nl>
Onderwerp: FW:

FYI een update van de statussen.

Tevens laat ik nog specifiek navragen of het wachtwoord wel klopte bij personen die nu aangeven dat ze het wachtwoord gewijzigd hebben.
Bovendien laat ik navragen of dat dan het wachtwoord was voor inloggen bij de OU, of bijv social media/LinkedIn etc.

Wordt vervolgd

Grt

FG

Van:
Verzonden: woensdag 25 november 2020 15:19
Aan: FG; F); Privacyofficer; S
Onderwerp: Via e-mail verzenden: CERT Wachtwoorden.xlsx
Bijlagen: CERT Wachtwoorden.xlsx

Allen,

Bij deze de recentste update.

Grtz,

Medewerkers		Opmerking
		Teams bericht verzonden
	?907a	Gemaild
		Teams bericht verzonden
		Teams bericht verzonden
		Teams bericht verzonden
		Teams bericht verzonden
		Teams bericht verzonden
		Teams bericht verzonden
		Teams bericht verzonden
	06e101	Gemaild
		Teams bericht verzonden
		Teams bericht verzonden
		Teams bericht verzonden
		Teams bericht verzonden
	3106	Teams bericht verzonden
		Gemaild

Respons
Wachtwoord klopt niet
Wachtwoord is aangepast
Wachtwoord klopt niet
Wachtwoord klopt niet
Wachtwoord klopt niet
Wachtwoord klopt niet
Wachtwoord klopt niet
Wachtwoord klopt niet
Wachtwoord is aangepast
Wachtwoord wordt al 5 jaar niet meer gebruikt
Wachtwoord klopt niet
Wachtwoord klopt niet
Wachtwoord klopt niet
Wachtwoord klopt niet
Wachtwoord klopt niet

Wachtwoord ooit eerder gebruikt of bij andere websites?
Gebruikte het wachtwoord vele-jaar geleden (Kan geen tijdsbestek aangeven). Gebruikte het wachtwoord en veranderd het cijfer ieder jaar. Vanaf maart/april dit jaa
Voor de zekerheid het wachtwoord gewijzigd (had het wachtwoord nog nooit gebruikt)
Nee, wachtwoord nog nooit gebruikt.
Nee, wachtwoord nog nooit gebruikt.
Nee, wachtwoord nog nooit gebruikt.
Nee, wachtwoord nog nooit gebruikt.
Nee, wachtwoord nog nooit gebruikt.
Voor de zekerheid het wachtwoord gewijzigd (had het wachtwoord nog nooit gebruikt)
Wachtwoord wordt al 5 jaar niet meer gebruikt
Geen antwoord via mail, niet via Teams bereikbaar. Telefoonnummer [redacted]rd niet opgenomen.
Nee, wachtwoord nog nooit gebruikt.
Nee, wachtwoord nog nooit gebruikt.
Nee, wachtwoord nog nooit gebruikt.
Nee, wachtwoord nog nooit gebruikt.
Nee, wachtwoord nog nooit gebruikt.
Geen antwoord via mail, niet via Teams bereikbaar. Telefoonnummer onbekend

ır komt het wachtwoord niet meer voor bij zijn OU-account. Heeft het wachtwoord mogelijk ook bij zijı ' gebruikt. Dit kan c

lie niet met zekerheid zeggen

Ontvangstbevestiging

Uw verzoek tot het indienen van een melding wordt in behandeling genomen.
U kunt de melding niet online raadplegen. Maak daarom een print voor uw eigen administratie. Doe dit voordat u deze pagina afsluit. Na het afsluiten van deze pagina zijn de gegevens die u heeft opgegeven niet meer beschikbaar. Onder het onderstaande meldingsnummer is de melding bekend bij de Autoriteit Persoonsgegevens. U heeft het meldingsnummer nodig om de melding aan te kunnen passen of in te kunnen trekken. Vermeld het meldingsnummer bij eventuele correspondentie met de Autoriteit Persoonsgegevens over de melding.

Tijdstip ontvangst	27-11-2020 10:42:51
Uniek nummer	

0. Over deze melding

Gaat het om een nieuwe of bestaande melding?	Een nieuwe melding indienen
Op grond van welke wettelijke bepaling doet u deze melding?	Algemene verordening gegevensbescherming (AVG)

1. Contactgegevens en overige algemene informatie

1.1 Contactgegevens

Over welke organisatie of welk bedrijf gaat het?

Registratienummer bij de Kamer van Koophandel	14128608
Naam van het bedrijf of de organisatie	Open Universiteit
Adres	Valkenburgerweg 177
Postcode	6401DL
Plaats	Heerlen

In welke sector is de organisatie of het bedrijf actief?	Onderwijs - Tertiair onderwijs
Overige sector, te weten:	Universiteit

Wie meldt het datalek?

Naam	
Functie	Functionaris voor de gegevensbescherming
E-mailadres	FG@ou.nl
Telefoonnummer	
Tweede telefoonnummer	

Met wie kan de Autoriteit Persoonsgegevens contact opnemen voor nadere informatie over de melding?

De melder is contactpersoon	Ja

1.2 Betrokkenheid andere organisatie

Was er een andere organisatie betrokken bij de inbreuk?	Ja, namelijk:
Naam van de andere organisatie die betrokken was bij de inbreuk	online forum cit0day

In welke hoedanigheid was de andere organisatie betrokken bij de inbreuk?
online forum genaamd 'cit0day', dat gericht is op het verkopen van gestolen gebruikersnamen en wachtwoorden, heeft een inbraak gehad op zijn eigen database

2. Tijdlijn

Exacte datum waarop de inbreuk was, indien bekend	23-11-2020
Einddatum van de periode waarbinnen de inbreuk was	26-11-2020
Duurt de inbreuk op dit moment nog voort?	Nee
Wanneer werd de inbreuk ontdekt?	25-11-2020
Als u de inbreuk later meldt dan 72 uur na de ontdekking, wat is daarvan dan de reden?	n.v.t.

3. Gegevens over het datalek

3.1 Aard van de inbreuk

Inbreuk op de vertrouwelijkheid van de gegevens	Ja
Inbreuk op de integriteit van de gegevens	Nee
Inbreuk op de beschikbaarheid van de gegevens	Nee

3.2 Aard van het incident

Wat is de aard van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest?	Hacking, malware (bijv. ransomware) en/of phishing

Geef een samenvatting van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest

cit0day heeft een inbraak gehad op zijn eigen database. Hierdoor liggen van 29 medewerkers van de Open Universiteit de gebruikersnaam en wachtwoord op straat (normaal moeten gebruikers cit0day betalen voor deze gegevens). De inschatting is dat ongeveer 35% van de gebruikersnaam/wachtwoord combinaties niet eerder op de website vermeld stonden. Van 12 medewerkers kan niet worden vastgesteld of er in het verleden sprake is geweest van misbruik, deze medewerkers zijn al geruime tijd uit dienst. De gebruikersnaam bestaat niet meer. Van 2 medewerkers kan niet worden vastgesteld of er is geweest van misbruik, deze medewerkers hebben niet gereageerd op het vragen van de OU - aannemelijk is dat zij het wachtwoord hebben gewijzigd. Van 1 medewerker kan niet worden vastgesteld of er is geweest van misbruik, deze medewerker is inmiddels uit dienst. Het wachtwoord werd door ICT gereset. Van 2 medewerkers is duidelijk geworden dat zij het wachtwoord in het verleden (ongeveer 5 jaren geleden) hebben gebruikt, maar dat dit wachtwoord inmiddels niet meer juist is. Van 12 medewerkers werd vastgesteld dat zij dit wachtwoord nooit gebruikt hebben voor hun OU-account. Met gebruikersnaam/wachtwoordwoord kan toegang verkregen worden tot de omgeving medewerker.ou.nl (dit betreft een extra handeling), waarbinnen de gebruiker toegang krijgt tot het personeelsdossier (beperkt), de salarisadministratie, de SURFfilesender-omgeving en het algemene profiel van de medewerker De gebruikersnaam/wachtwoordwoord werden mogelijk al

geruime tijd gepubliceerd op de website van cit0day. De OU heeft geen reden om aan te nemen dat er in het verleden misbruik werd gemaakt van deze gegevens, nu zich geen medewerkers hebben gemeld. De OU heeft onderzoek verricht om te kunnen vaststellen of er recent misbruik heeft plaatsgevonden, waarbij één incident werd geregistreerd (toegang tot account via IP-adres in Bratislava). Of hier daadwerkelijk sprake is van misbruik werd nog niet vastgesteld. Misbruik is niet aannemelijk nu duidelijk is geworden dat in vele gevallen het géén juist wachtwoord betrof én betreft, noch dat medewerkers dit wachtwoord ooit hebben gebruikt voor hun OU account. Dit maakt dat het niet aannemelijk is dat deze gegevens zijn verkregen via de OU. Het datalek is ten einde nu vast is komen te staan dat de gebruikersnaam niet meer bestond, het wachtwoord niet juist was of het wachtwoord is gewijzigd.

4. Persoonsgegevens die betrokken zijn bij het datalek

4.1 Persoonsgegevens in het algemeen

Naam	Ja
Geslacht, geboortedatum en/of leeftijd	Ja
Burgerservicenummer (BSN)	Nee
Contactgegevens	Ja
Toegangs- of identificatiegegevens	Ja
Financiële gegevens	Ja
(Kopieën van) paspoorten of andere legitimatiebewijzen	Nee
Locatiegegevens	Nee
Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen	Nee

4.2 Bijzondere categorieën van persoonsgegevens

Persoonsgegevens waaruit iemands ras of etnische afkomst blijkt	Nee
Persoonsgegevens waaruit iemands politieke opvattingen blijken	Nee

Persoonsgegevens waaruit iemands religieuze of levensbeschouwelijke overtuigingen blijken	Nee
Persoonsgegevens waaruit iemands lidmaatschap van een vakbond blijkt	Nee
Gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid	Nee
Gegevens over iemands gezondheid	Nee
Genetische gegevens	Nee
Biometrische gegevens	Nee

4.3 Hoeveelheid persoonsgegevens

Geef (eventueel bij benadering) aan hoeveel gegevensrecords ("gegevensregisters") zijn getroffen door de inbreuk	0

5. De groep mensen van wie persoonsgegevens betrokken zijn bij het datalek

Werknemers	Ja
Klanten (huidig en potentieel)	Nee
Leerlingen of studenten	Nee
Patiënten	Nee
Minderjarigen	Nee
Personen uit kwetsbare groepen	Nee

Omschrijf de groep mensen van wie persoonsgegevens zijn betrokken bij de inbreuk.
dwarsdoorsnede van 29 medewerkers van de OU. Deze medewerkers zijn niet gekoppeld aan hetzelfde organisatieonderdeel.

Van minimaal hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?	17
Van maximaal hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?	29

6. Maatregelen die zijn getroffen voordat het datalek plaatsvond

Waren de persoonsgegevens op het moment dat de inbreuk zich voordeed versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk voor onbevoegden?	Nee
Als de persoonsgegevens deels onbegrijpelijk of ontoegankelijk waren, om welk deel gaat dat dan?	n.v.t.

Als de persoonsgegevens geheel of deels onbegrijpelijk of ontoegankelijk waren gemaakt, op welke manier is dit dan gebeurd?

n.v.t.

7. Gevolgen van het datalek

7.1 Gevolgen van de inbreuk op de vertrouwelijkheid, de integriteit en/of de beschikbaarheid van de gegevens.

Onbevoegden hebben kennis kunnen nemen van de gegevens	Ja
De gegevens kunnen op een onbehoorlijke of onrechtmatige manier worden misbruikt	Ja
Er worden binnen uw eigen organisatie mogelijk onjuiste, onvolledige of achterhaalde persoonsgegevens gebruikt	Nee
Er worden mogelijk onjuiste, onvolledige of achterhaalde persoonsgegevens hergebruikt voor andere doeleinden of doorgegeven aan andere organisaties	Nee
Een essentiële dienst kan tijdelijk niet meer worden verleend aan de betrokkenen	Nee

FG

Van: FG
Verzonden: vrijdag 27 november 2020 14:36
Aan: ; Privacyofficer;
CC:
Onderwerp: datalek gemeld

Dag collega's,

Dank voor alle informatie en de tijd die jullie hierin hebben gestoken.
Ik heb vanmorgen (binnen de termijn van 72 uur) het datalek gemeld, met daarbij een beschrijving van alle overwegingen. Het risico acht ik verwaarloosbaar.

Daarbij was met name relevant het onderscheid tussen onjuiste wachtwoorden, oude wachtwoorden en de gevallen waarbij we niet hebben kunnen vaststellen of het een onjuist/ongeldig wachtwoord betrof. Het risico zat hem in de laatste 2 varianten. Ik zie geen aanleiding om aan te nemen dat er sprake is geweest van misbruik. Indien misbruik wél heeft plaatsgevonden, is dit nu niet meer mogelijk omdat de wachtwoorden (daar waar nodig) inmiddels zijn gewijzigd.

Met vriendelijke groet,

| functionaris gegevensbescherming

Werkdagen: maandag, dinsdag, woensdag en donderdag

Human resources, juridische zaken en inkoop | Juridische Zaken
bezoekadres: Valkenburgerweg 177 Heerlen | ATH 2.22
postadres: Postbus 2960 6401 DL Heerlen
I E FG@ou.nl

Please consider the environment and do not print this email unless absolutely necessary. Encourage environmental awareness.

-----Oorspronkelijk bericht-----
Van:
Verzonden: woensdag 25 november 2020 15:19
Aan: FG <fg@ou.nl>; I
<privacyofficer@ou.nl>
Onderwerp: Via e-mail verzenden: CERT Wachtwoorden.xlsx

Allen,

Bij deze de recentste update.

Grtz,

Westen, Saskia van der

Van: FG
Verzonden: woensdag 25 november 2020 11:13
Aan: . Privacyofficer
Onderwerp: FW: [SURFcert#106753] Gelekte gebruikersnamen - wachtwoorden

Ter info

Van:
Verzonden: woensdag 25 november 2020 08:55
Aan: FG <fg@ou.nl>
CC:

Onderwerp: RE: [SURFcert#106753] Gelekte gebruikersnamen - wachtwoorden

Ik zie drie opties:

- Voorlopig melden omdat we binnen 72 uur niet alle personen zullen bereiken om te vragen of het ooit een geldig wachtwoord bij de OU was en of zij (met enig risico voor betrokkenen) persoonsgegevens verwerk(t)en;
- Melden omdat wij er met redelijke zekerheid van uit kunnen gaan dat er (van de 29) gebruikers op de lijst meerdere gebruikers persoonsgegevens verwerkt zullen hebben. Helemaal zeker zullen we het nooit weten, één gebruiker meldt immers dat het wachtwoord als 5 jaar niet meer in gebruik is. Dat betekent dat sommige accounts (en wachtwoorden) al dusdanig oud zijn dat medewerkers uit dienst zullen zijn en we die nooit zullen bereiken.
- Niet melden omdat volstrekt onduidelijk is of er enig risico voor de OU en betrokkenen is geweest (zijn het ooit geldige accounts en wachtwoorden bij de OU geweest) en er geen signalen zijn van misbruik.

Ik lees (en weet, uit de pers) nog niet van signalen van misbruik. Tenzij er high profile (student- of medewerkersadministratie) gebruikers tussen zitten is de kans op schade voor betrokkenen mijns inziens klein tot verwaarloosbaar. Mijn suggestie is daarom: Uit voorzorg melden aan AP zonder voorlopige melding (extra werk, echt nieuwe bruikbare informatie niet te verwachten) zodat AP weet dat wij actief ontwikkelingen volgen. Verbeterpunten (waar nog nodig): awareness en multi factor authenticatie.

Heb je iets aan deze aanvullende overwegingen? Ik verwacht overigens niet dat de OU loggings heeft waarin van 5 jaar geleden of langer nog zinvolle informatie te halen is. Dat zou ook niet passend zijn, loggings moeten niet langer dan een half jaar tot jaar aanwezig blijven.

Groet,

Van: FG <fg@ou.nl>
Verzonden: dinsdag 24 november 2020 12:53
Aan:
CC:
Onderwerp: RE: [SURFcert#106753] Gelekte gebruikersnamen - wachtwoorden

Dag

Morgen zal ik mijn standpunt met jou delen, in ieder geval dat er sprake is van een datalek (met mogelijk een aantal overwegingen). Hierover kunnen we een gesprek voeren en afhankelijk van de uitkomst, stappen we morgen samen naar het Cvb. Het informeren van het Cvb doe ik het liefst ook morgen (i.v.m. de termijn van 72 uur).

Met vriendelijke groet,

... | functionaris gegevensbescherming

Werkdagen: maandag, dinsdag, woensdag en donderdag

Human resources, juridische zaken en inkoop | Juridische Zaken
bezoekadres: Valkenburgerweg 177 Heerlen | ATH 2.22
postadres: Postbus 2960 6401 DL Heerlen
E FG@ou.nl

Open Universiteit

FG

Van: FG
Verzonden: woensdag 25 november 2020 09:26
Aan:
CC:
Onderwerp: RE: [SURFcert#106753] Gelekte gebruikersnamen - wachtwoorden

Dag

De AP heeft in het verleden het standpunt ingenomen dat indien we misbruik niet kunnen uitsluiten, er toch gemeld moet worden. Deze lijn volg ik graag. Zeker nu gisteren tijdens een overleg met de AP waarbij de AP ook duidelijk heeft aangegeven dat dergelijke gevallen altijd gemeld moeten worden.

De overige overwegingen zijn natuurlijk terecht, deze zal ik verwoorden op het meldingsformulier. Het standpunt omtrent de risico's voor betrokkenen deel ik, zeker omdat er geen signalen zijn van misbruik.

Met vriendelijke groet,

tionaris gegevensbescherming

Werkdagen: maandag, dinsdag, woensdag en donderdag

Human resources, juridische zaken en inkoop | Juridische Zaken
bezoekadres: Valkenburgerweg 177 Heerlen | ATH 2.22
postadres: Postbus 2960 6401 DL Heerlen
| E FG@ou.nl

Open Universiteit

Van:
Verzonden: woensdag 25 november 2020 08:55
Aan: FG <fg@ou.nl>
CC:

Onderwerp: RE: [SURFcert#106753] Gelekte gebruikersnamen - wachtwoorden

Hi

Ik zie drie opties:

- Voorlopig melden omdat we binnen 72 uur niet alle personen zullen bereiken om te vragen of het ooit een geldig wachtwoord bij de OU was en of zij (met enig risico voor betrokkenen) persoonsgegevens verwerk(t)en;
- Melden omdat wij er met redelijke zekerheid van uit kunnen gaan dat er (van de 29) gebruikers op de lijst meerdere gebruikers persoonsgegevens verwerkt zullen hebben. Helemaal zeker zullen we het nooit weten, één gebruiker meldt immers dat het wachtwoord als 5 jaar niet meer in gebruik is. Dat betekent dat sommige accounts (en wachtwoorden) al dusdanig oud zijn dat medewerkers uit dienst zullen zijn en we die nooit zullen bereiken.
- Niet melden omdat volstrekt onduidelijk is of er enig risico voor de OU en betrokkenen is geweest (zijn het ooit geldige accounts en wachtwoorden bij de OU geweest) en er geen signalen zijn van misbruik.

Ik lees (en weet, uit de pers) nog niet van signalen van misbruik. Tenzij er high profile (student- of medewerkersadministratie) gebruikers tussen zitten is de kans op schade voor betrokkenen mijns inziens klein tot verwaarloosbaar. Mijn suggestie is daarom: Uit voorzorg melden aan AP zonder voorlopige melding (extra werk, echt nieuwe bruikbare informatie niet te verwachten) zodat AP weet dat wij actief ontwikkelingen volgen. Verbeterpunten (waar nog nodig): awareness en multi factor authenticatie.

Heb je iets aan deze aanvullende overwegingen? Ik verwacht overigens niet dat de OU loggings heeft waarin van 5 jaar geleden of langer nog zinvolle informatie te halen is. Dat zou ook niet passend zijn, loggings moeten niet langer dan een half jaar tot jaar aanwezig blijven.

Groet,

Van: FG <fg@ou.nl>
Verzonden: dinsdag 24 november 2020 12:53
Aan:
CC:
Onderwerp: RE: [SURFcert#106753] Gelekte gebruikersnamen - wachtwoorden

Dag

Morgen zal ik mijn standpunt met jou delen, in ieder geval dat er sprake is van een datalek (met mogelijk een aantal overwegingen). Hierover kunnen we een gesprek voeren en afhankelijk van de uitkomst, stappen we morgen samen naar het Cvb. Het informeren van het Cvb doe ik het liefst ook morgen (i.v.m. de termijn van 72 uur).

Met vriendelijke groet,

:n | functionaris gegevensbescherming

Werkdagen: maandag, dinsdag, woensdag en donderdag

Human resources, juridische zaken en inkoop | Juridische Zaken
bezoekadres: Valkenburgerweg 177 Heerlen | ATH 2.22
postadres: Postbus 2960 6401 DL Heerlen
:l | E FG@ou.nl

Open Universiteit

FG

Van: FG
Verzonden: woensdag 25 november 2020 11:02
Aan:
Onderwerp: contact met Cvb volgt

Dag

hebben besloten het onderzoek voort te zetten, zodat we op het moment van het doen van de melding zeker weten dat het datalek ten einde is.
Het Cvb informeren we dan ook pas morgen later op de dag, of vrijdag in de ochtend.

Met vriendelijke groet,

functionaris gegevensbescherming

Werkdagen: maandag, dinsdag, woensdag en donderdag

Human resources, juridische zaken en inkoop | Juridische Zaken
bezoekadres: Valkenburgerweg 177 Heerlen | ATH 2.22
postadres: Postbus 2960 6401 DL Heerlen
E FG@ou.nl

Open Universiteit

FG

Van:
Verzonden: maandag 30 november 2020 20:46
Aan: FG
CC: ; Cert;
Onderwerp: FW: Gestolen gebruikersnamen en wachtwoorden

Hoi

Onderstaand nog de reactie van die op de lijst stond.
Hij heeft vorige week nog zijn wachtwoord veranderd.
Maar zoals hij aangeeft is dit een wachtwoord dat hij totaal niet herkent.

Grt

Van:
Verzonden: maandag 30 november 2020 20:41
Aan:
CC:
Onderwerp: RE: Gestolen gebruikersnamen en wachtwoorden

Hallo

Dat wachtwoord herken ik helemaal niet. Misschien iets uit de begintijd van de OU-mail? Dan hebben we het over begin jaren negentig. Maar nee, dit komt mij niet bekend voor. Dus zeker de laatste twintig jaar niet gebruikt, zeer waarschijnlijk nooit.
Ik gebruik voor elke service een ander wachtwoord, dus (ook) niet gebruikt voor webshops of social media.
Wat ik wel vreemd vind is dat het forum dus wachtwoorden verkoopt, terwijl die incorrect zijn.
Hartelijke groet,

Van
Verzonden: maandag 30 november 2020 20:24
Aan:
CC:
Onderwerp: Gestolen gebruikersnamen en wachtwoorden

Hallo

Hierbij dan de info:

Een online forum genaamd 'cit0day', dat gericht is op het verkopen van gestolen gebruikersnamen en wachtwoorden, heeft een inbraak gehad op zijn eigen database. Normaal gesproken moet er periodiek betaald worden om een update te krijgen van de wachtwoorden, nu liggen ze allemaal publiek op straat.

Vwb jouw account staat vermeld:

De vraag is dus: herken je dit wachtwoord? Zo ja, heb je dit gebruikt om in te loggen bij de OU? Zo ja, van wanneer tot wanneer? Of heb je het account en wachtwoord gebruikt voor bijv webshops of social media?

Bedankt, grt

Open Universiteit
www.ou.nl

Dienst Informatietechnologie en facilitaire zaken
bezoekadres: Valkenburgerweg 177 Heerlen
postadres: Postbus 2960 6401 DL Heerlen

FG

Van: FG
Verzonden: woensdag 17 maart 2021 13:38
Aan:
Onderwerp: RE: [SURFcert#106753] Gelekte gebruikersnamen - wachtwoorden
Bijlagen: 2020-11-24 SURFcert rev FG.docx

Dag !

Bijgaand mijn aanvullingen.

Met vriendelijke groet,

Werkdagen: maandag, dinsdag, woensdag en donderdag

Human resources, juridische zaken en inkoop | Juridische Zaken
bezoekadres: Valkenburgerweg 177 Heerlen | ATH 2.22
postadres: Postbus 2960 6401 DL Heerlen
G@ou.nl

Open Universiteit

Van:
Verzonden: maandag 15 maart 2021 16:07
Aan: FG <fg@ou.nl>
Onderwerp: RE: [SURFcert#106753] Gelekte gebruikersnamen - wachtwoorden

Hi

Ik herinner me dat Jan en jij dit als datalek bespraken met het CvB en jij gemeld hebt bij de AP. Had jij hierover ook een afrondend advies geschreven dat ik aan de call kan toevoegen alvorens deze geheel te sluiten? (Inderdaad, ietwat achterstallig werk, ik kan nog niet heel lang in Marval ;-))

Met vriendelijke groet,

Informatietechnologie en facilitaire zaken | Innovatie en development

Open Universiteit
www.ou.nl

bezoekadres: Valkenburgerweg 177 Heerlen
postadres: Postbus 2960 6401 DL Heerlen

Van: FG <fg@ou.nl>
Verzonden: woensdag 25 november 2020 09:26
Aan: [redacted] >
CC:

Onderwerp: RE: [SURFcert#106753] Gelekte gebruikersnamen - wachtwoorden

Dag [redacted]

De AP heeft in het verleden het standpunt ingenomen dat indien we misbruik niet kunnen uitsluiten, er toch gemeld moet worden. Deze lijn volg ik graag. Zeker nu gisteren tijdens een overleg met de AP [redacted] waarbij de AP ook duidelijk heeft aangegeven dat dergelijke gevallen altijd gemeld moeten worden.

De overige overwegingen zijn natuurlijk terecht, deze zal ik verwoorden op het meldingsformulier. Het standpunt omtrent de risico's voor betrokkenen deel ik, zeker omdat er geen signalen zijn van misbruik.

Met vriendelijke groet,

[redacted] | functionaris gegevensbescherming

Werkdagen: maandag, dinsdag, woensdag en donderdag

Human resources, juridische zaken en inkoop | Juridische Zaken
bezoekadres: Valkenburgerweg 177 Heerlen | ATH 2.22
postadres: Postbus 2960 6401 DL Heerlen
[redacted] | **E** FG@ou.nl

Open Universiteit

Van: [redacted] >
Verzonden: woensdag 25 november 2020 08:55
Aan: FG <fg@ou.nl>
CC:
[redacted]
Onderwerp: RE: [SURFcert#106753] Gelekte gebruikersnamen - wachtwoorden

Hi

Ik zie drie opties:

- Voorlopig melden omdat we binnen 72 uur niet alle personen zullen bereiken om te vragen of het ooit een geldig wachtwoord bij de OU was en of zij (met enig risico voor betrokkenen) persoonsgegevens verwerk(t)en;
- Melden omdat wij er met redelijke zekerheid van uit kunnen gaan dat er (van de 29) gebruikers op de lijst meerdere gebruikers persoonsgegevens verwerkt zullen hebben. Helemaal zeker zullen we het nooit weten, één gebruiker meldt immers dat het wachtwoord als 5 jaar niet meer in gebruik is. Dat betekent dat sommige accounts (en wachtwoorden) al dusdanig oud zijn dat medewerkers uit dienst zullen zijn en we die nooit zullen bereiken.
- Niet melden omdat volstrekt onduidelijk is of er enig risico voor de OU en betrokkenen is geweest (zijn het ooit geldige accounts en wachtwoorden bij de OU geweest) en er geen signalen zijn van misbruik.

Ik lees (en weet, uit de pers) nog niet van signalen van misbruik. Tenzij er high profile (student- of medewerkersadministratie) gebruikers tussen zitten is de kans op schade voor betrokkenen mijns inziens klein tot verwaarloosbaar. Mijn suggestie is daarom: Uit voorzorg melden aan AP zonder voorlopige melding (extra werk, echt nieuwe bruikbare informatie niet te verwachten) zodat AP weet dat wij actief ontwikkelingen volgen. Verbeterpunten (waar nog nodig): awareness en multi factor authenticatie.

Heb je iets aan deze aanvullende overwegingen? Ik verwacht overigens niet dat de OU loggings heeft waarin van 5 jaar geleden of langer nog zinvolle informatie te halen is. Dat zou ook niet passend zijn, loggings moeten niet langer dan een half jaar tot jaar aanwezig blijven.

Groet,

Van: FG <fg@ou.nl>
Verzonden: dinsdag 24 november 2020 12:53
Aan:
CC: '
Onderwerp: RE: [SURFcert#106753] Gelekte gebruikersnamen - wachtwoorden

Dag .

Morgen zal ik mijn standpunt met jou delen, in ieder geval dat er sprake is van een datalek (met mogelijk een aantal overwegingen). Hierover kunnen we een gesprek voeren en afhankelijk van de uitkomst, stappen we morgen samen naar het Cvb. Het informeren van het Cvb doe ik het liefst ook morgen (i.v.m. de termijn van 72 uur).

Met vriendelijke groet,

ı | functionaris gegevensbescherming

Werkdagen: maandag, dinsdag, woensdag en donderdag

Human resources, juridische zaken en inkoop | Juridische Zaken
bezoekadres: Valkenburgerweg 177 Heerlen | ATH 2.22
postadres: Postbus 2960 6401 DL Heerlen
| E FG@ou.nl

Open Universiteit

Marval #
SURFcert #
IP 145.20.xxx.

[SURFcert#106753] Gelekte gebruikersnamen - wachtwoorden

24-11-2020

Op 23-11 ontvingen we onderstaande mail van SURFcert:

Beste CERT-OUNL,

== Waarom ontvangt u deze mail ==

Een online forum genaamd 'cit0day', dat gericht is op het verkopen van gestolen gebruikersnamen en wachtwoorden, heeft een inbraak gehad op zijn eigen database. Normaal gesproken moet er periodiek betaald worden om een update te krijgen van de wachtwoorden, nu liggen ze allemaal publiek op straat. Hierbij zitten ook accounts van Uw instelling. De inschatting is dat ongeveer 35% van de gebruikersnaam/wachtwoord combinaties nog niet in eerdere publicaties zijn geweest. Hieronder de link waarmee de wachtwoorden van Uw organisatie te downloaden zijn.

Er is niet meer info over waar de accounts oorspronkelijk gestolen zijn, of hoe lang dat geleden is.

== Downlad link ==

https://cernbox.cern.ch/index.php/s/8oj4a95JQudgGxs

== Wat verwacht SURFcert nu van jullie ==

Willen jullie van de betreffende accounts onderzoeken of de wachtwoorden nog geldig zijn en passende maatregelen nemen?
SURFcert zal het ticket sluiten, het hoeft niet afgemeld te worden.

== Openstaande incidenten ==

Hieronder staan eventueel de incidenten vermeld die op dit moment nog openstaan voor jullie instelling:
--

Met vriendelijke groeten,

SURFcert Officer on Duty
--
SURFcert . cert@SURFnet.nl . https://surf.nl/surfcert phone (24/7): . PGP: 0x4bc9be47bd783d33

Marval #
SURFcert #
IP 145.20.xxx.

Overweging van de FG:

Op 23 november 2020 ontving de OU bericht dat het online forum 'Cit0day' gehackt is, waardoor van 29 medewerkers van de OU de accountnaam en het (veronderstelde) wachtwoord op staat lagen. Normaliter moet worden betaald voor deze gegevens.

De inschatting is dat ongeveer 35% van de gebruikersnaam/wachtwoord combinaties niet eerder op de website vermeld stonden. Van 12 medewerkers kan niet worden vastgesteld of er in het verleden sprake is geweest van misbruik, deze medewerkers zijn al geruime tijd uit dienst. De gebruikersnaam bestaat niet meer. Van 2 medewerkers kan niet worden vastgesteld of er is geweest van misbruik, deze medewerkers hebben niet gereageerd op het vragen van de OU - aannemelijk is dat zij het wachtwoord hebben gewijzigd.

Van 1 medewerker kan niet worden vastgesteld of er is geweest van misbruik, deze medewerker is inmiddels uit dienst. Het wachtwoord werd door ICT gereset. Van 2 medewerkers is duidelijk geworden dat zij het wachtwoord in het verleden (ongeveer 5 jaren geleden) hebben gebruikt, maar dat dit wachtwoord inmiddels niet meer juist is. Van 12 medewerkers werd vastgesteld dat zij dit wachtwoord nooit gebruikt hebben voor hun OU-account. Met gebruikersnaam/wachtwoordwoord kan toegang verkregen worden tot de omgeving medewerker.ou.nl (dit betreft een extra handeling), waarbinnen de gebruiker toegang krijgt tot het personeelsdossier (beperkt), de salarisadministratie, de SURFfilesender-omgevingen het algemene profiel van de medewerker De gebruikersnaam/wachtwoordwoord werden mogelijk al geruime tijd gepubliceerd op de website van cit0day. De OU heeft geen reden om aan te nemen dat er in het verleden misbruik werd gemaakt van deze gegevens, nu zich geen medewerkers hebben gemeld. De OU heeft onderzoek verricht om te kunnen vaststellen of er recent misbruik heeft plaatsgevonden, waarbij één incident werd geregistreerd (toegang tot account via IP-adres in Bratislava). Of hier daadwerkelijk sprake is van misbruik werd nog niet vastgesteld. Misbruik is niet aannemelijk nu duidelijk is geworden dat in vele gevallen het géén juist wachtwoord betrof én betreft, noch dat medewerkers dit wachtwoord ooit hebben gebruikt voor hun OU account.

Niet kan worden vastgesteld op welke wijze de wachtwoorden en accountnamen in beginsel verkregen zijn. Op dit moment bestaat geen aanleiding om aan te nemen dat deze wachtwoorden via een hack of op enige andere wijze via de OU zijn verkregen. Tijdens het onderzoek is duidelijk geworden dat een deel van de wachtwoorden (waarbij we dit met zekerheid hebben kunnen vaststellen) géén OU wachtwoorden betreffen, noch dat deze ooit zijn gebruikt door de medewerker op enige ander medium. De inbreuk werd op 23 november 2020 gesignaleerd en werd beëindigd op 26 november 2020.

Gelet op het kleine aantal medewerkers, kan niet anders worden aangenomen dat de wachtwoorden op andere wijze zijn verkregen. We kunnen bijvoorbeeld denken aan Linked-In.

Het datalek is ten einde nu vast is komen te staan dat de gebruikersnaam niet meer bestond, het wachtwoord niet juist was of het wachtwoord is gewijzigd.

De FG overweegt nu misbruik niet kan worden uitgesloten, er sprake is van een datalek. Zij volgt hierbij de strikte lijn die de AP hanteert. De FG zal een melding doen bij de AP, waarbij benadrukt wordt dat misbruik van de gegevens niet aannemelijk is, noch dat wij hier aanleiding voor hebben gezien. Overwogen wordt dat n onbevoegden kennis hebben kunnen nemen van de gegevens en dat gegevens op een onbehoorlijke of onrechtmatige manier kunnen worden misbruikt

Marval #
SURFcert #
IP 145.20.xxx.

Onderstaand de lijst van de accounts die het betreft:

	account bestaat niet meer
	account bestaat niet meer
	account bestaat niet meer
	account bestaat niet meer
	account bestaat niet meer
	account bestaat niet meer
	account bestaat niet meer
	account bestaat niet meer
	account bestaat niet meer
	account bestaat niet meer
	account bestaat niet meer
	account bestaat niet meer
	Wachtwoord gereset
	Wachtwoord klopt niet (meer)
	Wachtwoord is aangepast
	wachtwoord nooit gebruikt
	wachtwoord nooit gebruikt
	wachtwoord nooit gebruikt
	wachtwoord nooit gebruikt
	wachtwoord nooit gebruikt
	Wachtwoord is aangepast
	Wachtwoord wordt al 5 jaar niet meer gebruikt
01	Gemaild
	wachtwoord nooit gebruikt
	wachtwoord nooit gebruikt
	wachtwoord nooit gebruikt
	wachtwoord nooit gebruikt
	Gemaild

Van:
Verzonden: dinsdag 13 april 2021 21:20
Aan: FG <fg@ou.nl>
CC:
Onderwerp: Oud incident uit 2020: toen wel of niet behandeld (en gemeld) als datalek?

Hi

De verdachte inlog van collega vorig jaar december ontbrak op mijn incidentenrapportage. Was het behandeld als datalek en heb jij er een verslagje van dat ik aan de CERT rapportage kan toevoegen? In Marval kan ik er juist geen call van vinden, mogelijk omdat de Servicedesk er niet bij betrokken is geraakt.

Dank je en groet,

hief Information Security & Quality Officer

Informatietechnologie en facilitaire zaken | Innovatie en development
bezoekadres: Valkenburgerweg 177 Heerlen
postadres: Postbus 2960 6401 DL Heerlen

Open Universiteit
www.ou.nl

Van:
Verzonden: vrijdag 27 november 2020 09:30
Aan:

Onderwerp: RE: contact ivm melden datalek?

We gaan melden aan de AP.

Is onderstaande inlog op te volgen?

Van:
Verzonden: vrijdag 27 november 2020 09:13
Aan:

Onderwerp: Re: contact ivm melden datalek?

Heb nog even in onze MS Advanced Threat protectie logs gekeken voor alle users vanaf regel 14. Van deze users zijn 2 meldingen, waarvan 1 zorgelijk:
Atypical travel bij (maar dat kan ook VPN zijn, of device thuis terwijl op vakantie etc)

User's risk report | User's sign-ins | User's risky sign-ins | Linked risky sign-in

Detection type	Atypical travel	Activity	Sign-in
Risk state	At risk	Detection time	9/5/202(
Risk level	Medium	Detection last updated	9/5/202(
Risk detail	-	Token issuer type	Azure AI
Source	Identity Protection	Travel duration	4:43
Detection timing	Offline		

En (niet Atypical, maar nieuwe locaties, normaal gesproken niks mee aan de hand)

9/7/2020, 10:40:15 AM	145.20.80.4	Amst
9/1/2020, 9:38:15 AM	185.61.72.122	Bruss

Beide users zijn inmiddels ook al met 2FA uitgerold dus zouden nu ook de 2FA verplichting krijgen bij zo'n login.
heeft 2FA sinds 3-11, sinds 19-8

From: "
Date: Friday, 27 November 2020 at 08:45
To: '

Subject: FW: contact ivm melden datalek?

FYI, we gaan een overleg in met de CvB

Van: FG <fg@ou.nl>
Verzonden: vrijdag 27 november 2020 08:35
Aan:
Onderwerp: contact ivm melden datalek?

Dag

Ik sta nog steeds achter het melden van dit datalek, nu we een deel niet kunnen uitsluiten. De AP voert een vrij strikt beleid ten aanzien van het melden van dit soort zaken. Wel hebben we natuurlijk een sterk verhaal!
Wanneer zie jij tijd deze ochtend om samen het Cvb te contacteren? Mocht het niet mogelijk zijn om samen te gaan, dan kan ik (na eventuele afstemming) zelf naar het Cvb stappen.

Met vriendelijke groet,

unctionaris gegevensbescherming

Werkdagen: maandag, dinsdag, woensdag en donderdag

Human resources, juridische zaken en inkoop | Juridische Zaken
bezoekadres: Valkenburgerweg 177 Heerlen | ATH 2.22
postadres: Postbus 2960 6401 DL Heerlen
E FG@ou.nl

Open Universiteit