Van:
Verzonden: vrijdag 19 juni 2020 11:26
Aan:
CC: FG
Onderwerp: 2020-06-04 Twee laptops gestolen uit auto

Hallo
Ter informatie.
We hebben bovenstaand incident gesloten, maar als je nog nieuwe info krijgt, willen we die uiteraard graag hebben.

V.w.b. datalek onderscheiden we de volgende 3 categorieën:

* Er kan niet worden uitgesloten dat bij het incident onrechtmatige verwerking van persoonsgegevens heeft plaatsgevonden.
A Het incident is bij de AP gemeld als datalek.
B Bij het incident zijn bovendien de betrokkenen geïnformeerd.

Deze is door de FG geclassificeerd als *.
==========
Met vriendelijke groet,

Marval #30842
SURFcert #
IP 145.20.xxx.

2020-06-04 Twee laptops gestolen uit auto.docx

4-6-2020 Medewerker meldt dat gisteren 03-06-2020 om ca. 16:30 uur twee Apple laptops met tag nrs A14374 en A14898 zijn gestolen uit zijn auto terwijl deze geparkeerd stond bij een AH filiaal. Van beide laptops waren de schijven versleuteld, maar de apparaten waren niet uitgeschakeld. Het is dus mogelijk dat de dief ze heeft gedetecteerd aan de hand van hun radio-signalen. Alle accounts van zijn geblokkeerd en inmiddels zijn de wachtwoorden van die accounts aangepast. Beide systemen zijn niet meer online geweest na de diefstal. Hoewel voor beide systemen via iCloud een vergrendelopdracht is verstuurd, wordt die pas uitgevoerd als de systemen weer online komen. Zolang de systemen offline blijven, is het ook niet mogelijk om via de Apple dienst "Zoek mijn ..." hun positie te bepalen.

Van de diefstal is aangifte gedaan.

TAG-nummer	Serienummer	Merk	Model	Fabrikantnummer	Kleur
		Apple	MacBook Pro (15-inch, 2018)	MR942N/A	Grijs
		Apple	MacBook Pro (16-inch, 2019)	MVVK2N/A	Grijs

11-06-2020 geeft aan dat beide systemen zodanig waren ingericht dat het wachtwoord moet worden ingevuld alvorens de systemen – als zij standy zijn, bijvoorbeeld omdat de deksel is gesloten – weer gebruikt kunnen worden.

12-06-2020 FG

Het onderzoek heeft voldoende uitgewezen dat onrechtmatige toegang tot OU gegevens, pas kan worden verkregen nadat zowel het wachtwoord van de Apple laptop wordt ingevoerd én het IDM wachtwoord van de OU account wordt ingevoerd. De accounts zijn spoedig geblokkeerd.

Verder valt op te merken dat Apple gebruik maakt van een bijzondere vorm van 2FA, waarbij inlogpogingen vanaf een ongebruikelijke client of IP-adres worden herkend. De eigenaar van het iCloud account wordt in zo'n geval geïnformeerd, en gevraagd te verifiëren of hijzelf diegene is die probeert in te loggen.

Toegang tot het OU account middels een van de gestolen laptops is uitsluitend mogelijk als de dader – naast het wachtwoord van de laptop – ook beschikt over de VPN authenticatie (2FA) van ófwel kan inloggen op het netwerk van de OU. Pas dan krijgt de dader toegang tot potentieel waardevolle informatie. Daarbij kan worden opgemerkt dat wanneer het systeem verbinding maakt met een bekend netwerk (zo ook het OU netwerk), de vergrendelopdracht alsnog worden uitgevoerd.

In zijn algemeenheid valt op te merken dat de schijven zeer goed beveiligd zijn, waarbij de kans dat deze gekraakt worden nagenoeg 0 is.

Uit bovenstaande is gebleken dat de verkrijger van de laptop over meerdere wachtwoorden dient te beschikken om toegang te kunnen krijgen tot de OU omgeving die potentieel waardevolle informatie (en p-gegevens) bevat. Geoordeeld kan worden dat beveiligingswaarborgen zijn getroffen, hetgeen met zich meebrengt dat de diefstal een laag risico met zich mee brengt. Anders zou dit zijn wanneer schijven minder goed beveiligd zouden zijn, of volstaan kan worden met het (mogelijk kunnen) invoeren van één wachtwoord. De FG is van mening dat hier geen sprake is van een datalek dat aan de AP gemeld zou moeten worden.

Van:
Verzonden: woensdag 10 juni 2020 11:54
Aan: FG
CC: Privacyofficer
Onderwerp: RE: 30842, Macbooks: A14374 en A14898 gestolen van

Hallo '
Ik heb gesproken, en denk dat ik de meeste van je vragen kan beantwoorden. Maak maar een afspraak (of gebruik die van).

Van: FG <fg@ou.nl>
Verzonden: zondag 7 juni 2020 18:01
Aan: ; Privacyofficer <privacyofficer@ou.nl>
Onderwerp: RE: 30842, Macbooks: A14374 en A14898 gestolen van

Dag

Ik zou graag weer een afspraak inplannen om een algemene uitleg over het 'systeem' te krijgen . De zaken die ik graag wil begrijpen heb ik met blauw gearceerd.

Met betrekking tot de specifieke casus het volgende (waarbij ik adviseer om eerst dit bericht te lezen, alvorens te scrollen naar geel en groen)
Algemene opmerkingen heb ik met geel gearceerd (zie mails hieronder). Een tegenstelling heb ik met groen gearceerd (zie mails hieronder). Met rood gemarkeerd de vragen die voor mij nog open staan en met roze een vraag die volgens mij – bij nader inzien – niet meer relevant is.

Bij diefstal is het zeer aannemelijk dat het de dieven gaat om de waarde van de apparaten, niet om de content. Ik heb begrepen . Dit maakt niet dat we er geen aandacht aan hoeven besteden, maar maakt wellicht wel dat indien de versleuteling adequaat is we niet (zo snel) hoeven te spreken van een datalek zoals de AP dit bedoelt.

Indien de laptop op slaapstand stond en het zo heeft ingesteld dat je dan een wachtwoord moet invoeren, spreek ik al van een vergrendeling.

- Vragen of dit zo had ingesteld – dit lijkt me essentieel. Indien dit niet zo ingesteld was, verliest de stelling "er is geen toegang meer verkregen tot het account" alle kracht. Toegang tot het account betekent dat ww is ingevoerd, toch?
- Indien 'ja' op bovenstaande vraag in rood, vragen of een overwegend sterk wachtwoord had – wellicht is deze vraag niet meer relevant omdat 1) inmiddels het account is geblokkeerd/toegang gewijzigd (welke van de twee is dit, wil je dit uitleggen?) en 2) we weten dat geen toegang meer is verkregen tot account.
- Vragen of informatie op de D-drive, etc. had staan.

Indien de laptop vergrendeld was (immers slaapstand met wachtwoord (hoop ik)), begrijp ik niet zo goed wat de verstande "vergrendelopdracht" nog meer kan doen. Is dit een extra vergrendeling – wat wordt hier dan extra vergrendeld? Of is dit een actie, ervanuit gaande dat de laptop niet zo is ingesteld dat bij het dichtklappen ervan het wachtwoord opnieuw ingevoerd moet worden? (zie ook groen gearceerd, dit lijkt elkaar tegen te spreken).

1) Indien de laptop vergrendeld was, moet de dief en het (account)wachtwoord weten. [redacted]
   - In dat geval heeft de dief toegang tot de D-drive, downloads, het bureaublad, etc.
2) Indien de dief het (account)wachtwoord weet, bestaat de mogelijkheid dat de dief verbinding maakt met het OU netwerk.
   - In dat geval heeft de dief toegang tot de R-drive, Q-drive, M-drive, etc.
3) Indien de dief het (account)wachtwoord weet, moet de dief het [redacted] weten van de SSD's. [redacted]
   - In dat geval heeft de dief toegang tot de SSD's. [redacted]

Kortom alles staat of valt, met de instelling van het invoeren van een wachtwoord bij het dichtklappen van de laptop en/of het weten van het wachtwoord (in welk geval alsnog toegang verkregen kan worden). [redacted]

Groetjes,

Van:
Verzonden: vrijdag 5 juni 2020 14:31
Aan: FG <fg@ou.nl>; Privacyofficer <privacyofficer@ou.nl>
Onderwerp: Re: 30842, Macbooks: A14374 en A14898 gestolen van

Collega's,
Goede vragen want ook ik heb alleen via e-mail contact met gehad. Dus nog niet alles kunnen uitzoeken wat ik zou hebben willen weten.

Apple heeft een service die *Zoek mijn* heet. heeft de beide apparaten daarvoor aangemeld. Als je de wachtwoorden hebt, kun je de apparaten daarmee o.a. zoeken, wissen en vergrendelen. Die service stuurt dan over Internet een door jou gekozen opdracht naar het betreffende apparaat. Het apparaat voert die opdracht uit.

Inmiddels is opgemerkt dat die service alleen werkt als de apparaten internettoegang hebben. (De US politiediensten hebben procedures over in beslag genomen Apple apparatuur). Dus als je ze meteen uitzet of in een kooi van Faraday bewaart of zo, dan gebeurt er niets (volgens mij kan ik zelfs thuis gaan zitten met de laptops nog 'aan', maar voer ik niet het wifi wachtwoord in -- ook dan gebeurt er niets). Het is dus een gok of de dief de apparaten alleen heeft uitgezet om ze te verkopen of dat deze mogelijkheden onderzoekt om de inhoud te kunnen benaderen. De harde schijf is versleuteld en de accounts van zijn geblokkeerd, dus m.i. gaat dat niet lukken.

Een laptop kan online komen als die is ingeschakeld en in het bereik komt van een netwerk waarvoor deze geautoriseerd is: OU Wifi, Eduroam, s wifi thuis of andere voor het apparaat bekende netwerken.

Zie verder in rood beneden.

Van: FG <fg@ou.nl>
Verzonden: vrijdag 5 juni 2020 12:18
Aan: .vacyofficer <privacyofficer@ou.nl>
Onderwerp: RE: 30842, Macbooks: A14374 en A14898 gestolen van

Dag collega's,

Ik ben een beetje bevooroordeeld én heb vertrouwen in het onderzoek dat reeds heeft plaatsgevonden (CERT heeft dit soort zaken vaker gezien). Toch een aantal vragen zodat ik de systematiek beter begrijp en een kritische noot.

Ik lees: "[redacted] of is dit de Cloudomgeving (of is dit bij Apple hetzelfde)? Vervolgens lees ik dat deze opdracht pas uitgevoerd kan worden als de systemen weer online komen. Met online komen zal bedoeld worden dat de laptops verbinding maken met internet Ja (dit kan mogelijk door een locatie van de OU te betreden? Ja). Ik interpreteer dit als: de laptops worden pas vergrendeld wanneer de laptop verbinding maakt met het netwerk van de OU, dit vind ik natuurlijk een beetje spannend... M.i. terecht.
Wat zijn de (mogelijke) gevolgen van het nog niet kunnen uitvoeren de vergrendelopdracht?
Wat wil ik graag weten:

1) Waren de laptops vergrendeld
   > is voor mij niet helemaal duidelijk [redacted]
2) Is nog toegang verkregen na diefstal
   > volgens mij niet geeft ook aan van niet
3) Kan alsnog toegang worden verkregen (dit vraag ik i.v.m. het nog niet kunnen uitvoeren van de vergrendelopdracht)
   > volgens mij wel... Alleen als je het wachtwoord weet én de machine van het netwerk houdt tot je de kans hebt gehad de instellingen te wijzigen. De kans dat je de laptop van het netwerk houdt lijkt me vrij groot, ik hoop dat de kans dat je het wachtwoord weet erg klein is...
4) Staan er bestanden op locaties anders dan de vergrendelde (nog niet vergrendeld, maar wel versleuteld) schijven.
   > hier heb ik niks van gezien n gaf aan dat hij daar nog over na ging denken, maar de resultaten daarvan heb ik nog niet gekregen.

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

Van:
Verzonden: vrijdag 5 juni 2020 08:53
Aan: Privacyofficer <privacyofficer@ou.nl>; FG <fg@ou.nl>
Onderwerp: Re: 30842, Macbooks: A14374 en A14898 gestolen van

Collega's,

Hierbij de bijgewerkte versie van de beschrijving van het incident *2020-06-04 Twee laptops gestolen uit auto*.

Als de FG rechtstreeks met zou willen overleggen, houd CERT dan s.v.p. in de loop.

In de CERT registratie moeten we ook nog opnemen welke klasse qua datalek de FG hieraan toekent.

Van: Privacyofficer <privacyofficer@ou.nl>
Verzonden: vrijdag 5 juni 2020 08:01
Aan:
Onderwerp: FW: 30842, Macbooks: A14374 en A14898 gestolen van

Hoi

Heb jij gisteren nog meer duidelijkheid gekregen rondom de diefstal van de laptops? Is sprake van dataverlies en de kans op een datalek? Dit wordt sowieso in het incidentenregister opgenomen; ik vraag dit omdat we dit ook moeten melden aan FG?

Met vriendelijke groet,

Human resources, Juridische zaken en Inkoop | Juridische zaken
bezoekadres: Valkenburgerweg 177 Heerlen, 6419 AT Heerlen
gebouw Athabasca, kamer 2.07
postadres: Postbus 2960 6401 DL Heerlen
T 045 - 576 29 12

Open Universiteit
www.ou.nl

35JAAR

Van: Servicedesk, Fenl <servicedesk@ou.nl>
Verzonden: donderdag 4 juni 2020 09:19
Aan: Privacyofficer <privacyofficer@ou.nl>
CC:
Onderwerp: RE: 30842, Macbooks: A14374 en A14898 gestolen var

Beste

In de call staat dat de admin-accounts van geblokkeerd zijn. Beide Macbooks zijn via iCloud vergrendeld en de SSD's zijn versleuteld.
Ik heb via Teams gevraagd of die verdere acties kan ondernemen.

Met vriendelijke groet,

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

Open Universiteit
www.ou.nl

35JAAR

Van: Privacyofficer <privacyofficer@ou.nl>
Verzonden: donderdag 4 juni 2020 09:09
Aan: Servicedesk, Fenl <servicedesk@ou.nl>
CC:
Onderwerp: RE: 30842, Macbooks: A14374 en A14898 gestolen var

Beste collega,

Is deze melding ook al bekend bij CERT? Van belang is onder meer of sprake is van een datalek. Hiervoor is belangrijk te achterhalen of de laptops uitgeschakeld waren. Waren de laptops tevens geblokkeerd? Is na de diefstal nog toegang verschaft tot de laptops? Is het account van de collega tijdelijk geblokkeerd en is te achterhalen of men toegang heeft verschaft tot het account?

Alvast dank.

Met vriendelijke groet,

Human resources, Juridische zaken en Inkoop | Juridische zaken
bezoekadres: Valkenburgerweg 177 Heerlen, 6419 AT Heerlen
gebouw Athabasca, kamer 2.07
postadres: Postbus 2960 6401 DL Heerlen
T 045 - 576 29 12

Open Universiteit
www.ou.nl

35JAAR

Van: Servicedesk <servicedesk@ou.nl>
Verzonden: donderdag 4 juni 2020 08:17
Aan: Privacyofficer <privacyofficer@ou.nl>
Onderwerp: 30842, Macbooks: A14374 en A14898 gestolen van

Open Universiteit
www.ou.nl

Call toewijzing

Call met meldingsnummer INC-30842 is aan jou toegewezen.
Het betreft: Macbooks: A14374 en A14898 gestolen van

Met vriendelijke groet,

Servicedesk
Facilitaire en IT-voorzieningen
tel. 045-5762306
e-mail: servicedesk@ou.nl

FG

Van:
Verzonden: donderdag 4 juni 2020 09:54
Aan: FG
CC:
Onderwerp: Gestolen laptops
Bijlagen: 2020-06-04 Twee laptops gestolen uit auto.docx

Hallo
Hierbij informatie over een nieuw incident.

==========
Met vriendelijke groet,

Marval #30842
SURFcert #
IP 145.20.xxx.

2020-06-04 Twee laptops gestolen uit auto.docx

4-6-2020 Medewerker neldt dat gisteren 03-06-2020 om ca. 16:30 uur twee Apple laptops met tag nrs A14374 en A14898 zijn gestolen uit zijn auto terwijl deze geparkeerd stond bij een AH filiaal. Van beide laptops waren de schijven versleuteld, maar de apparaten waren niet uitgeschakeld. Het is dus mogelijk dat de dief ze heeft gedetecteerd aan de hand van hun radio-signalen. Beide systemen zijn via iCloud vergrendeld en de accounts van zijn geblokkeerd.

Van de diefstal is aangifte gedaan.

Bij I nagevraagd hoe laat de systemen vergrendeld zijn en of er met " Zoek mijn ..." nog iets te vinden is over de huidige locatie.

Marval #30842
SURFcert #
IP 145.20.xxx.

2020-06-04 Twee laptops gestolen uit auto.docx

4-6-2020 Medewerker meldt dat gisteren 03-06-2020 om ca. 16:30 uur twee Apple laptops met tag nrs A14374 en A14898 zijn gestolen uit zijn auto terwijl deze geparkeerd stond bij een AH filiaal. Van beide laptops waren de schijven versleuteld, maar de apparaten waren niet uitgeschakeld. Het is dus mogelijk dat de dief ze heeft gedetecteerd aan de hand van hun radio-signalen. De accounts van zijn geblokkeerd. Beide systemen zijn niet meer online geweest na de diefstal. Hoewel voor beide systemen via iCloud een vergrendelopdracht is verstuurd, wordt die pas uitgevoerd als de systemen weer online komen. Zolang de systemen offline blijven, is het ook niet mogelijk om via de Apple dienst "Zoek mijn ..." hun positie te bepalen.

Van de diefstal is aangifte gedaan.

TAG-nummer	Serienummer	Merk	Model	Fabrikantnummer	Kleur
		Apple	MacBook Pro (15-inch, 2018)	MR942N/A	Grijs
		pple	MacBook Pro (16-inch, 2019)	MVVK2N/A	Grijs