Van:
Aan: FG; .
Cc:
Onderwerp: RE: Whatsapp gehacked.
Datum: maandag 9 november 2020 16:18:20

Hoi,

Eén aanvulling op onderstaande mail (groen gearceerd).

Grt,

Van: J
Verzonden: maandag 9 november 2020 14:07
Aan: FG <fg@ou.nl>; Privacyofficer <privacyofficer@ou.nl>
CC: M
Onderwerp: RE: Whatsapp gehacked.

Hoi

Ik zal proberen antwoorden te geven.

, vul/corrigeer svp waar nodig.

Grt

Van: FG <fg@ou.nl>
Verzonden: maandag 9 november 2020 14:02
Aan:
CC:
Onderwerp: RE: Whatsapp gehacked.

Dag

Mark en ik hebben hier net kort over gesproken, namens ons een aantal vragen:

- Om hoeveel gehackte medewerkers gaat het? -> geen idee, H heeft het gemeld en hij heeft 1200 contacten. Verder heb ik alleen gehoord M
- Zijn van al deze medewerkers de WhatsApp-accounts verwijderd (zoals de e-mail van ITF beschrijft)?-> van weten we dit, voor de rest weten wij niet wie/wat/hoe, vandaar de oproep/alert via mail naar iedereen.
- Ging het om zakelijke of privétoestellen?-> van is zakelijk
- Weten we hoe de personen zijn gehackt (social hacking, het klikken op een link of bekijken van video die een virus bevat)? -> nee, geen idee, gehackt via het sturen van die code zoals in de beschrijving staat.
- Heeft de hack zich verspreid via één medewerker?-> ook geen idee, ik weet niet of we

die aanname moeten doen. Maar heeft het gemeld en heeft vele contacten. Maar deze manier van hacken is niet raar in de whatsapp wereld.

- Weten we wanneer het is gebeurd?-> vandaag
- Zijn er gevallen bekend waarbij misbruik gemaakt is?-> nee
- Is het waarschijnlijk dat de hack/het virus zich via WhatsApp nestelt in het toestel zelf? Deze vraag stel ik omdat ik het doel van een dergelijke hack niet goed kan overzien. Wellicht zou het advies ook moeten zijn om een reset van het toestel uit te voeren (terug naar fabrieksinstellingen)?->het gaat om whatsapp en in de mailing is beschreven hoe hiermee om te gaan.
  Je weet natuurlijk nooit wat iemand allemaal in appverkeer zet..
  Nee, het is niet waarschijnlijk dat de hack zich via WhatsApp nestelt in het toestel zelf. Het uitvoeren van een reset van het toestel lijkt mij in deze gevallen daarom zeker niet nodig.
  Uiteraard is het ook mogelijk om via WhatsApp berichten met linkjes naar frauduleuze websites te ontvangen. Als je hierop klikt dan kun je ransomware binnenhalen op jouw toestel. Dit is identiek aan de werkwijze op bv. Windows-laptops.
  Er zijn zelfs gevallen waarbij de smartphone wordt vergrendeld nadat je op een dergelijk linkje hebt geklikt (geld betalen voor ontgrendelcode, etc...het bekende verhaal).
  Maar zoals aangegeven, dat is in dit geval niet aan de orde.

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

Open Universiteit

Van: J
Verzonden: maandag 9 november 2020 12:09
Aan: FG <fg@ou.nl>; Privacyofficer <privacyofficer@ou.nl>

CC: !
Onderwerp: FW: Whatsapp gehacked.

FYI, het mailtjes op dit moment opgesteld en gaat dan naar de hele organisatie.

Van: !
Verzonden: maandag 9 november 2020 11:51
Aan: Servicedesk, ITF <servicedesk@ou.nl>
CC: !
Onderwerp: FW: Whatsapp gehacked.

Beste collega's,

Mijn WhatsApp account is gehackt en dat van verschillende collega's ook.
Wat er gebeurt is dat je een WhatsApp bericht krijgt van 'zogenaamd mij' met de vraag om de code die je in een SMS bericht hebt ontvangen via WhatsApp te retourneren. Als je dat doet wordt ook jouw WhatsApp account gehackt.
Doe dat dus niet!
Ik zou voorstellen om hiervan een alert te laten uitgaan.

Met vriendelijke groet,

Onderwijsservices (OS)
bezoekadres: Valkenburgerweg 177 Heerlen
postadres: Postbus 2960 6401 DL Heerlen

Open Universiteit
www.ou.nl

Marval #30842Marval #<>
SURFcert #
IP 145.20.xxx.IP <>

2020-11-09 WhatsApp medewerker gehackt.docx

9-11-2020 Medewerker meldt op 9 november 2020 om 11:51 dat zijn WhatsApp account is gehackt. Het betreft de WhatsApp account, zoals geïnstalleerd op zijn zakelijke toestel. Op dit toestel bevinden zich 1200 contacten. Vanuit de WhatsApp account van de gehackte medewerker worden contacten via WhatsApp verzocht om de code die de ontvanger via SMS heeft ontvangen, via WhatsApp 'terug' te zenden naar de WhatsApp account van de gehackte medewerker. Ontvangers die deze handeling verrichten zijn/worden vervolgens ook gehackt. Diverse medewerkers van de OU hebben gehoor gegeven aan het bericht dat werd verstuurd via de WhatsApp account van medewerker , de WhatsApp accounts van medewerkers werden vermoedelijk ook gehackt.

9-11-2020 Om 12:09 werden de FG en PO door geïnformeerd.

9-11-2020 Om 12:36 werd door ITF het volgende e-mailbericht verzonden naar alle collega's:

Op dit moment zijn één of meerdere WhatsApp accounts van OU-medewerkers gehackt.
Op het moment dat een WhatsApp account is gehackt, kan degene vanuit jouw account berichten versturen.

Hoe zijn de WhatsApp accounts gehackt?
Je krijgt een bericht van een (gehackt nummer van een) bekende met een verzoek om de 'code die je straks ontvangt via SMS' door te sturen via WhatsApp. Het verhaal is meestal dat het per ongeluk naar jouw nummer is gestuurd.
Met deze code wordt er ingelogd op jouw WhatsApp account en je account is overgenomen.

Wat moet je doen om dit te voorkomen?
De allerbeste tip: reageer **niet op dit bericht en verwijder dit direct!**

Het je toch gereageerd en de code doorgestuurd, dan moet je direct onderstaande stappen ondernemen:

1) Verwijder WhatsApp van je telefoon.
2) Zet je telefoon uit en weer aan.
3) Download de WhatsApp app opnieuw vanuit de Playstore of Appstore.
4) Je logt vervolgens opnieuw in op je WhatsApp account met je telefoonnummer en vraagt een verificatiecode aan.
   Zodra je deze code hebt ontvangen én ingevoerd, wordt degene die zich heeft ingelogd op jouw account (de hacker) automatisch uitgelogd.

Het kan gebeuren dat je nu ook nog wordt gevraagd om de tweestapsverificatiecode. Heb je dat niet dan heeft de hacker dat misschien ingesteld of de hacker heeft deze veranderd.
In dit geval moet je zeven dagen wachten voordat je kan inloggen zonder deze tweestapsverificatiecode.
Máár de andere persoon (hacker) wordt wel uitgelogd op jouw account, ook als je die tweestapsverificatiecode niet hebt.

Heeft u toch nog vragen naar aanleiding van dit bericht, kunt u contact opnemen met de Servicedesk, 045-5762306 (servicedesk@ou.nl).

9-11-2020 Om 14:02 uur hebben de FG en PO een aantal vragen geformuleerd.

9-11-2020 Om 14:07 uur heeft een reactie gegeven.

9-11-2020 Om 16:18 uur heeft en reactie gegeven.

16-11-2020 de FG heeft nader onderzoek verricht.

Het onderzoek heeft voldoende uitgewezen dat er sprake is geweest van social hacking, waarbij er geen aanleiding bestaat om aan te nemen dat sprake was van ransomware of verwijzingen naar frauduleuze websites. Het is niet waarschijnlijk dat de hack zich via WhatsApp nestelt in het toestel zelf, waardoor het uitvoeren van een reset van het toestel niet nodig lijkt.

Naar aanleiding van het e-mailbericht hebben we van diverse getroffen medewerkers bericht ontvangen dat zij diens WhatsApp account hebben verwijderd en opnieuw met verificatiecode hebben ingelogd waardoor de hacker automatisch werd uitgelogd.

De hackers hebben gedurende beperkte duur toegang gehad tot de WhatsApp account van de diverse medewerkers en daarmee ook tot een grote hoeveelheid contactgegevens (naam en telefoonnummer) via WhatsApp.

Geoordeeld kan worden dat er sprake is van een inbreuk op de vertrouwelijkheid, daar een onbevoegde toegang heeft gehad tot een grote hoeveelheid (2500+) persoonsgegeven c.q. namen en telefoonnummers.
Geoordeeld kan worden dat er sprake is geweest van inbreuk op de beschikbaarheid, daar de gehackte medewerker gedurende een korte periode geen toegang heeft gehad tot diens WhatsApp account. Toegang tot de contactenlijst ('het telefoonboek') bleef voor de medewerker wel mogelijk. De toegang tot de WhatsApp account kon eenvoudig hersteld worden.

De aard van de inbreuk	Er zijn geen persoonsgegevens gewist en/of gewijzigd. Wel is er toegang geweest tot persoonsgegevens door onbevoegden
De aard, gevoeligheid en omvang van de persoonsgegevens	Onbevoegden hebben slechts toegang gekregen tot de WhatsApp account van diverse medewerkers waarbinnen namen en telefoonnummers zichtbaar zijn (2500+).

Overweging waardoor niet gekomen kan worden tot het oordeel dat er sprake is van een hoog risico:

Discriminatie	bijvoorbeeld bij een datalek met gegevens over ras, geloof of seksuele geaardheid	N.v.t.
Identiteitsdiefstal of –fraude	Bijvoorbeeld bij een datalek met complete paspoortkopieën. Of het BSN in combinatie met andere persoonsgegevens.	De hacker heeft zich voorgedaan als medewerker en daarbij diverse contacten uit de contactenlijst bericht. Er is geen sprake van ransomware.
Financiële verliezen	bijvoorbeeld bij een datalek met creditcardgegevens waardoor het risico bestaat dat iemand online bestellingen kan plaatsen op kosten van een ander.	N.v.t.
Reputatieschade	bijvoorbeeld bij een datalek met gegevens over problematische schulden, verslaving of prestaties op het werk.	N.v.t.
Doorbreking van beroepsgeheim	bijvoorbeeld bij een datalek met medische gegevens.	N.v.t.

Het ongeoorloofd ongedaan maken van gepseudonimiseerde persoonsgegevens.		N.v.t.
Een aanzienlijk economisch of maatschappelijk nadeel.		N.v.t.
Een situatie waarbij de betrokken personen hun rechten en vrijheden niet kunnen uitoefenen. Of geen controle over hun persoonsgegevens kunnen uitoefenen.		Tijdelijk geen toegang tot diens eigen WhatsApp account, waarbij toegang eenvoudig weer verkregen kan worden
Datalek met strafrechtelijke persoonsgegevens.		N.v.t.
Datalek met bijzondere persoonsgegevens, dan wel met bijzondere kenmerken van een persoon.		N.v.t.
Datalek met informatie over persoonlijke aspecten, bedoeld om profielen op te stellen of te gebruiken. Met name als het gaat om profiling op basis van informatie over beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid, gedrag en locatie.		N.v.t.
Datalek met persoonsgegevens van kwetsbare groepen. Zoals gehandicapten, mensen die ziek zijn, kinderen en bejaarden.		N.v.t.
Datalek met een grote hoeveelheid persoonsgegevens en met gevolgen voor een hele grote groep mensen.		De hacker heeft mogelijk toegang gehad tot een grote hoeveelheid namen en telefoonnummers. De gevolgen van de hack zijn m.i. beperkt daar niet alle contacten gehackt worden en bovendien de hack slechts een beperkt aantal contacten target (pas bij het versturen van de code wordt de contactpersoon ook gehackt).

Marval #30842Marval #<>
SURFcert #
IP 145.20.xxx.IP <>

16-11-2020 de FG is van mening dat de ernst en de risico's met betrekking tot het incident beperkt zijn. Voorts is zij van mening dat de organisatie haar medewerkers deugdelijk heeft geïnformeerd, waarbij ook duidelijk is geworden dat de gehackte medewerkers de toegang tot diens WhatsApp account met een simpele handeling 'terug' krijgen.
Het incident kan worden gesloten.