Andre Elings

Van: Cert (NCSC-NL) [cert@ncsc.nl]
Verzonden: maandag 21 juli 2014 15:26
Aan: Andre Elings
Onderwerp: RE: Hulpvraag i.v.m. verdachte inlog Digi-D / RE: "Handreiking cybercrime"

Beste heer Elings,

Naar aanleiding van uw e-mail d.d. 30 juni 2014 sturen wij u dit bericht.

In uw e-mail gaat u in op het antwoord van het NCSC, d.d. 26 juni 2014. U reageert onder meer op de term DDoS . Wij kunnen niet met zekerheid zeggen dat u de aanval die u zegt te ervaren een DDoS aanval betreft. Deze inschatting is gemaakt naar aanleiding van het contact dat wij met u hebben gehad. Voor het vaststellen van het exacte type aanval waarvan u last zegt te ondervinden, kunt u het beste contact opnemen met uw service provider. Wanneer er inderdaad sprake is van een aanval, zijn er verschillende gespecialiseerde bedrijven die u bij de afhandeling van uw incident kunnen ondersteunen. Het NCSC biedt alleen ondersteuning aan overheidsorganisaties en bedrijven die vitale diensten in Nederland leveren. Het NCSC kan u derhalve niet verder helpen.

Tot slot geeft u aan aangifte te hebben gedaan van de aanval bij de politie. Wij adviseren u om in contact te blijven met de politie. Wij hopen u tot slot met onze publicaties, waarvan de links in onze eerdere e-mails aan u vermeld werden, zo goed als mogelijk te hebben geholpen.
Met vriendelijke groet,
NCSC

-----Original Message-----
From: Andre Elings [mailto:andre@digi-d.nl]
Sent: maandag 30 juni 2014 14:52
To: Cert (NCSC-NL)
Cc: Stijn Handgraaf (NCSC-NL)
Subject: RE: Hulpvraag i.v.m. verdachte inlog Digi-D / RE: "Handreiking cybercrime"

Beste heer De Hamer,

Dank voor uw e-mail. Op een aantal punten ervan wil ik graag nog wat nader ingaan.

- U schrijft dat het om een DDos-aanval gaat; ikzelf wist niet dat het een DDos-aanval was, mij is daar door de politie ook niets over gezegd.

- De informatie ontvangen wij niet alleen via onze website maar ook rechtstreeks per mail en ook via onze statistieken.

- Wij slaan de gegevens niet op op onze server, de gegevens worden dagelijks gedurende een werkweek verwijderd nadat we ze offline hebben weggeschreven naar een externe harde schijf. Het verwijderen van gegevens in onze statistieken is niet mogelijk. Bovendien denk ik dat zelfs de van de server verwijderde gegevens door een hacker/techneut achterhaald zouden kunnen worden.

- Ik vind het jammer en teleurstellend dat het NCSC niets voor ons kan betekenen. Ik denk namelijk dat dit juist wel een cybersecurity probleem is waar u ons bij zou kunnen helpen. Dat maak ik ook op uit uw website (o.a. bij '24-uurshulp'). Het feit dat onze site wordt aangevallen en er mogelijk wordt geprobeerd om digidcodes, bestemd voor de overheid, te 'pakken' maakt het onmiskenbaar een cybersecurity probleem. Het gaat om bescherming van aan de staat toevertrouwde en voor deze bestemde gegevens tegen een aanval; dat deze gegevens vertrouwelijk zijn en onderwerp van onderzoek van het CBP maakt dat niet anders.

Het is een aanval op een systeem waar gegevens binnenkomen die voor de overheid zijn bedoeld en dat maakt het naast een privacy-probleem absoluut ook een cybersecurity-probleem, zeker nu we al een paar keer zijn aangevallen. Ook het binnenkomen van dergelijke data via url-strings van ons statistiekenprogramma duidt op een groot probleem; ook hiervoor geldt dat deze data zijn bedoeld voor de overheid en niettemin bij ons terechtkomen. Graag zouden we hulp en ondersteuning krijgen om dit tegen te gaan en wij verzoeken u dan ook vriendelijk om uw besluit om ons niet te helpen nog eens te overwegen.

CC dhr. S. Handgraaf

Met vriendelijke groeten,

André Elings
M +31 6 547 811 27
E andre@digi-d.nl

Logo en huisstijl | Reclame | Webdesign | Mobiele websites | QR Codes | Foto en tekst | Drukwerk | Sign | Beursmateriaal

Prunusstraat 21
5143 AS WAALWIJK the Netherlands

T +31 416 - 56 39 23
F +31 416 - 56 39 27
I www.digi-d.nl

KvK Tilburg 18129710

-----Oorspronkelijk bericht-----
Van: Cert (NCSC-NL) [mailto:cert@ncsc.nl]
Verzonden: donderdag 26 juni 2014 10:39
Aan: Andre Elings
Onderwerp: RE: Hulpvraag i.v.m. verdachte inlog Digi-D / RE: "Handreiking cybercrime"

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

Beste heer Elings,

Hartelijk dank voor uw bericht. Zoals dinsdag besproken, bij deze een mail over hoe het NCSC kan bijdragen bij het verhelpen van de twee incidenten waarmee u te maken heeft. Allereerst bent u het slachtoffer van een DDoS aanval op uw website. Hiernaast ontvangt u gevoelige en persoonlijke informatie, die bestemd is voor www.digid.nl.

Voor wat betreft het eerste, hiervoor geeft u aan in contact te zijn met de politie en zij zijn bezig met een onderzoek. Wij adviseren u om in contact te blijven met de politie over het verloop en de uitkomst van dit onderzoek. Voor nadere informatie over dit type aanvallen voor nu en in de toekomst, verwijs ik u naar onze factsheet hierover: https://www.ncsc.nl/dienstverlening/expertise-advies/factsheets/factsheet-continuiteit-van-online-diensten.html

Het tweede verschijnsel is geen cybersecurity probleem, het is een privacy probleem. U geeft aan gevoelige informatie van derden te ontvangen, die tot u komt via systemen van externe partijen. Niet alleen laten gebruikers gegevens achter op uw website en e-mail, u geeft ook aan dat de gegevens verschijnen in uw statistieken. Deze informatie slaat up op in uw serverlogs en uw systemen en wanneer deze ten prooi zouden vallen aan een kwaadwillende, zorgen ze voor een groot probleem. Omdat het hier gaat over het lekken van persoonsgegevens, is de partij die moet optreden het College Bescherming Persoonsgegevens (CBP). Zij zijn toezichthouder op het gebied van privacy en de manier waarop met persoonsgegevens moet worden omgegaan.
Ze hebben onder andere als taak: advisering, voorlichting, informatieverstrekking en verantwoording. Verder kunnen partijen die persoonsgegevens en gevoelige data lekken worden aangegeven bij deze partij.

U heeft aangegeven dat het CBP op woensdag 25 juni bij u op bezoek komt.
Naast dat ze u kunnen helpen bij het omgaan met de gegevens die u zelf in bezit heeft, kunnen ze ook hulp bieden bij het verhelpen van het naar u lekken van gegevens door derden.

Omdat het NCSC en het CBP gescheiden organisaties zijn, kan het NCSC u niet ondersteunen in dit traject. De data waarmee het CBP en het NCSC werken is gevoelig en de zaken waarmee we werken worden gescheiden gehouden.

Ik hoop u hiermee voldoende te hebben geïnformeerd. Veel succes met de verdere afhandeling van het incident.

Met vriendelijke groet

Martijn de Hamer
NCSC

From: Andre Elings [mailto:andre@digi-d.nl]
Sent: donderdag 19 juni 2014 10:57
To: Stijn Handgraaf (NCSC-NL)
Cc: rt@tickets.ncsc.nl
Subject: Hulpvraag i.v.m. verdachte inlog Digi-D / RE: "Handreiking cybercrime"

Geachte heer Handgraaf,

Telefonisch heb ik u eerder geïnformeerd dat er een gerichte aanval vorige week op onze website www.digi-d.nl is gedaan.
Gisteren hebben wij na een verdachte inlog voor de zekerheid onze statistieken bekeken en kwamen een verdacht IP adres tegen (zie screenshots hieronder).

Wij maken ons ernstige zorgen in deze situatie, kunt u ons adviseren en hulp bieden?
We hebben namelijk meer activiteiten op onze website uit diverse Oostbloklanden, Rusland en China.

Onderstaande de inlog die is binnengekomen.

cid:image002.jpg@01CF8B17.5A0D3F40

IP adres: 193.150.120.14

cid:image004.jpg@01CF8B17.5A0D3F40

Locatie Ip adres 193.150.120.14 Rusland!
cid:image015.jpg@01CF8B17.5A0D3F40

Betreffend Ip adres 193.150.120.14 staat gerapporteerd als Hacking, Spoofing en Spam!

http://www.abuseipdb.com/report-history/193.150.120.14

cid:image016.jpg@01CF8B17.5A0D3F40

Met vriendelijke groeten,

André Elings

M +31 6 547 811 27

E andre@digi-d.nl

Prunusstraat 21

5143 AS WAALWIJK the Netherlands

T +31 416 - 56 39 23

F +31 416 - 56 39 27

I www.digi-d.nl

KvK Tilburg 18129710

Algemene voorwaarden Digi-D v.o.f.

DISCLAIMER

Dit e-mailbericht inclusief eventuele bijlagen, kan vertrouwelijke informatie bevatten en is alleen bestemd voor de persoon of instantie aan wie het e-mailbericht is gericht. Indien U niet de beoogde ontvanger bent, verzoeken wij U de afzender te informeren en het e-mailbericht te verwijderen. Het is verboden om dit e-mailbericht of de inhoud te gebruiken, publiceren of te distribueren. Op alle transacties en diensten zijn de algemene voorwaarden van toepassing, waarin een aansprakelijkheidsbeperking is opgenomen. De voorwaarden zijn in te zien op de website en worden op verzoek toegezonden.

This e-mail message including attachments, if any, may contain confidential material and is intended only for the person or entity to which it is addressed. If you are not the intended recipient please notify the sender immediately and then delete this e-mail. Any unauthorized use, disclosure or distribution of this e-mail is prohibited. The partnership's general conditions, which contain a limitation of liability, are applicable to all transactions and services. The conditions can be viewed on the website and will be provided upon request.

- -----Oorspronkelijk bericht-----
Van: Stijn Handgraaf (NCSC-NL) [mailto:[redacted]
Verzonden: donderdag 12 juni 2014 13:12
Aan: Andre Elings
CC: rt@tickets.ncsc.nl
Onderwerp: "Handreiking cybercrime"

Geachte heer André Elings,

Naar aanleiding van het telefonisch gesprek van deze ochtend stuur ik bij deze de "Handreiking cybercrime" toe ter ondersteuning bij aangifte bij de politie:

https://www.ncsc.nl/actueel/nieuwsberichten/publicatie-cybercrime.html
<https://www.ncsc.nl/actueel/nieuwsberichten/publicatie-cybercrime.html>

Het document is een handreiking voor overheden, bedrijfsleven, opsporingsambtenaren en burgers om cybercrime te herkennen en er aangifte van te doen.

Bijlage F omschrijft een Checklist voor vaststellen en aangifte.

In bijlage H staat een Stappenplan veiligstellen van digitale sporen omschreven.

Met vriendelijke groet,

Stijn Handgraaf

Security Specialist

.....
...

Nationaal Cyber Security Centrum

Postbus 117 | 2501 CC| Den Haag | www.ncsc.nl <http://www.ncsc.nl>
.....
...

Tel 070 888 75 55 Email [redacted]
<mailto:[redacted]
.....
...

-----BEGIN PGP SIGNATURE-----
[redacted]