Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2017–2018

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 548

BRIEF VAN DE STAATSSECRETARIS VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 29 juni 2018

Op vrijdag 22 juni heeft het Fraudeteam van Logius (de beheerder van DigiD en MijnOverheid) door een melding vastgesteld dat valse MijnOverheid e-mails zijn verstuurd. Burgers die op de link in deze e-mails hebben geklikt, zijn doorgeleid naar een valse MijnOverheid website, met een vals DigiD-inlogscherm. De gegevens van de burgers die hebben geprobeerd in te loggen, zijn in handen gekomen van onbevoegde personen.

Ik neem deze zaak zeer hoog op. In een situatie waarin iedereen steeds vaker gevraagd wordt zijn zaken digitaal te doen, is phishing een criminele activiteit die de digitalisering ondermijnt en mensen rechtstreeks raakt.

Tijdens het mondelinge vragenuur van 26 juni jl. heeft de Minister over dit incident al kort met uw Kamer gesproken over de op dat moment bekende feiten (Handelingen II 2017/18, nr. 98, Mondelinge vragen van het lid Middendorp over het bericht «waarschuwing valse mails MijnOverheid»). Middels deze brief informeer ik u, mede namens de Minister van Justitie en Veiligheid, over de feiten die tot nu toe uit het nadere onderzoek naar voren zijn gekomen.

Hoe werkte deze phishing?

Er is een e-mail gestuurd met een link naar een malafide website. Deze website legde de hand op authenticatiegegevens, inclusief SMS van de getroffen burgers. Vervolgens werd direct en geautomatiseerd ingelogd bij MijnOverheid op de persoonlijke pagina van de ingelogde persoon, en werd deze doorzocht. Aannemelijk is dat er persoonsgegevens zijn verzameld. Naast de bekende 203 gevallen zijn er, voor zover nu bekend, geen gegevens van anderen in het geding geweest.

Samen met het NCSC (Nationaal Cyber Security Center) en NCTV (Nationaal Coördinator Terrorismebestrijding en Veiligheid) is geconsta-

kst-26643-548
ISSN 0921 - 7371
's-Gravenhage 2018

teerd dat deze phishing e-mails en phishing websites zeer goed zijn voorbereid en uitgevoerd. In de financiële dienstverlening zijn dergelijke geavanceerde phishing activiteiten al langer gaande. In de publieke dienstverlening is dit een nieuwe fase waartegen we ons moeten wapenen.

Feitenrelaas

Na het ontdekken is het protocol voor dit soort calamiteiten in gang gezet en heeft Logius vrijdagochtend 22 juni jl. direct de volgende acties ondernomen, in nauwe samenwerking met onder meer het NCSC en RvIG (Rijksdienst voor Identiteitsgegevens):

- Op vrijdag 22 en zaterdag 23 juni zijn twee malafide websites uit de lucht gehaald en is een waarschuwing breed gecommuniceerd.
- In het weekend hebben in totaal 1040 burgers melding gedaan van het ontvangen van verdachte mails.
- Op maandag 25 juni zijn 203 getroffen accounts verwijderd, nadat was onderzocht en vastgesteld welke DigiD-accounts getroffen waren. De betreffende personen zijn hierover op de hoogte gesteld door middel van een brief.
  Daarnaast is aangifte gedaan bij de Nationale Politie.
- Dinsdag 26 juni aan het einde van de middag, werd na vervolgonderzoek een aantal voorlopige bevindingen gedaan. Wanneer de betreffende burgers inlogden op de valse websites, werden de ingevoerde gegevens direct middels een script gebruikt om via DigiD in te loggen bij MijnOverheid. Na inloggen via een malafide script werd MijnOverheid doorzocht. In drie gevallen werd met succes 2-factor authenticatie toegepast. Aannemelijk hierbij is dat persoonsgegevens werden verzameld.
- Woensdag 27 juni aan het einde van de middag werden deze bevindingen bevestigd door het fraudeteam van Logius.

Verder hebben wij de volgende acties ondernomen:

- De Autoriteit Persoonsgegevens (AP) is op de hoogte gesteld van de phishing activiteit en het lekken van persoonlijke gegevens.
- Het RvIG is met het Centraal Meldpunt Identiteitsfraude- en fouten (CMI) betrokken als adviseur. Tevens ondersteunen zij in de communicatie met getroffen burgers.
- De ketenpartners UWV, Belastingdienst en SVB zijn op de hoogte gesteld.
- Er zijn verschillende activiteiten onderzocht om phishing verder te bemoeilijken. Op korte termijn wordt extra ingezet op monitoring en detectie. Voor de lange termijn worden verschillende technische maatregelen onderzocht.

Nadere maatregelen

Bij DigiD en MijnOverheid is reeds eerder een reeks van maatregelen getroffen. MijnOverheid stuurt zelf nooit mails met een link, juist om phishing te voorkomen en communiceert daarover voortdurend naar gebruikers. Het verkeer op de website MijnOverheid en DigiD wordt continu gemonitord. Snelle signalering door getroffen burgers is veelal de start van effectieve bestrijding. Uiteraard is alertheid van burgers nodig. Voorlichtingscampagnes over veilig internetten en het herkennen van phishing acties zijn daarop gericht.

Dit soort aanvallen is nooit 100% uit te sluiten. Ik laat samen met de Minister van Justitie en Veiligheid onderzoeken welke aanvullende acties nog meer mogelijk zijn om phishing verder te bemoeilijken, de veiligheid van gegevens te garanderen en tegelijkertijd de beschikbaarheid van

digitale overheidsdienstverlening te waarborgen. In de Nederlandse Cybersecurity Agenda (NCSA) heeft de Minister van Justitie en Veiligheid namens het kabinet reeds tal van maatregelen aangekondigd om de cyberveiligheid in Nederland naar een hoger plan te tillen.

Tot slot

Zoals aangegeven loopt het onderzoek naar dit incident door. De ernst van dit soort phishing activiteiten is evident. Voor de getroffen burgers en voor de overheid is het een ingrijpende gebeurtenis met mogelijke vervolgschade en onzekerheid. Identiteitsgegevens komen door phishing acties als deze in verkeerde handen, waarmee misbruik kan plaatsvinden. Dat willen we te allen tijde voorkomen.

Mocht het verdere onderzoek daartoe aanleiding geven, zal ik de Kamer uiteraard nader informeren over de uitkomsten ervan en over de vervolgacties.

De Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,
R.W. Knops