'Vendetta' dreigt accountgegevens klanten online te zetten en eist opheffen van downloadlimiet

Hacker chanteert Belgacom na 'kraken van internetmodems'

Een onbekende hacker heeft afgelopen maandagavond de accountgegevens van dertig internetklanten bij het telecombedrijf Belgacom online bekendgemaakt en dreigt er tegen het einde van november nog eens 285.000 vrij te geven. Hij eist dat Belgacom de download-limieten van zijn internetaanbod opheft.

DOOR RONALD MEEUS

BRUSSEL ● Belgacom diende ondertussen klacht in tegen de naar eigen zeggen Amerikaanse hacker, die zichzelf de naam Vendetta heeft toebedeeld. De Computer Crime Unit van de federale politie onderzoekt de zaak. De hacker zelf zegt dat hij een manier heeft gevonden om de internetmodems van Belgacom te kraken, maar dat wordt zowel door Belgacom als door onafhankelijke veiligheidsexperts betwijfeld.

Maandagavond om 22 uur dook er op de internetforums van adsl-bc.org, een vereniging van Franstalige Belgacom Skynet-gebruikers, ineens een lijst op met de gebruikersnaam en het wachtwoord van 30 internetabonnees van het telecombedrijf. Met een duidelijk dreigement erbij: Belgacom moet tegen 30 november zijn downloadlimieten opheffen of er komt een nieuwe lijst met liefst 285.000 buitgemaakte accountgegevens online. Om het dreigement nog wat kracht bij te zetten, opperde het bericht dat er volgende week, en alle weken daarna, samen nog eens duizend accounts te grabbel zullen worden gegooid om aan te tonen dat het hem menens is.

In een eerste reactie opperde Belgacom-woordvoerder Jan Margot nog dat er geen enkele indicatie bestond dat de gegevens echt waren. Maar gisternamiddag checkte het bedrijf alle publiek gemaakte gebruikersgegevens en die bleken allemaal echt te zijn. Wie ze in handen kreeg, kon zich dus toegang verschaffen tot de mailbox en de accountinstellingen van de gebruikers in kwestie. "We hebben onmiddellijk klacht ingediend tegen de persoon", reageert Margot. "Hij heeft het imago van ons bedrijf schade toegebracht en wat hij heeft gedaan – zich onrechtmatig toegang verschaffen tot onze gebruikersgegevens – wordt ook strafrechtelijk vervolgd. De dertig internetklanten hebben we ondertussen gecontacteerd en verzocht om dringend hun gebruikersgegevens te wijzigen."

Dreigement

In het bericht dat de hacker plaatste op de forums van adsl-bc.org claimt hij een Amerikaan te zijn die gedegouteerd is door de manier waarop de Belgische internetprovider met zijn klanten omgaat. Belgacoms adsl-klanten kunnen maandelijks 25 gigabyte aan gegevens downloaden, en dat is volgens een kleine groep internetgebruikers – waaronder dus duidelijk de hacker in kwestie – veel te

FOTO PHOTONEWS

■ Klanten bij een internetpakket van Belgacom. Daarmee kunnen ze elke maand 25 gigabyte downloaden; te weinig volgens de hacker.


Hacker chanteert Belgacom na 'kraken van internetmodems'

weinig. "Internet is een recht voor iedereen, dat niet moet worden beperkt", oppert hij in zijn bericht.

De hacker sluit af met erg strijdvaardige taal: een potpourri van citaten uit de mond van onder meer Martin Luther King, een paar strijdzinnen die altijd worden gebruikt door de internationale hackersbende Anonymous en tot slot een quote uit de film *Terminator 2*, waarin het computergestuurde booswicht toevallig, net als het internetmerk van Belgacom, Skynet heet: "We hebben Skynet bij de ballen."

De onvrede over downloadlimieten bestaat al jaren en wordt ook richting Belgacoms concurrent Telenet geuit. Beide bedrijven zetten een plafond op het aantal gegevens die een gebruiker maandelijks kan downloaden, in tegenstelling tot de meeste internetproviders in het buitenland. Maar slechts een kleine fractie van zware internetgebruikers wordt er echt door geraakt: Belgacom zegt dat het jaarlijks slechts enkele tienduizenden pakketten met extra ruimte om te downloaden verkoopt, op een totaal aantal abonnees van ongeveer anderhalf miljoen.

BBox2

"De eis van de hacker is niet echt in verhouding met wat hij heeft uitgehaald", zegt expert Eddy Willems van het beveiligingsbedrijf Kaspersky. "Want laat ons er geen doekjes om winden: dit is een ernstig misdrijf."

De zaak wordt momenteel onderzocht door de Computer Crime Unit van de federale politie. Ondertussen onderzocht Belgacom zelf ook hoe de hacker in kwestie de gegevens kan hebben losgeweekt. Zelf zegt hij dat hij zich toegang kan verschaffen tot de BBox2, de internetmodem van Belgacom. Daarop staan de logingegevens van de eigenaar opgeslagen, omdat de modem geregeld zelf inlogt bij de systemen van Belgacom. Maar volgens Margot werd er gisteren geen enkele aanwijzing gevonden dat er een programmeerfout zit in de interne software van de toestellen, die door eventuele hackers kan worden aangewend om het toestel te kraken.

EDDY WILLEMS (BEVEILIGINGSEXPERT):
Eis van hacker is niet in verhouding met wat hij heeft uitgehaald. Dit is een ernstig misdrijf

"Geen enkele technologie is onkraakbaar, dat hebben gebeurtenissen uit het verleden al aangetoond", zegt Willems. "Maar ik betwijfel ook dat de hacker die gegevens via het kraken van Belgacoms Bboxen heeft verkregen. Als er een 'exploit' zou zijn, een exploiteerbare fout in de programmatuur, zou Belgacom dat normaal gezien na een onderzoek moeten opmerken. Ook een andere relatief eenvoudige hackingmethode, phishing, lijkt me uitgesloten. Wie zich zijn gebruikersgegevens laat ontfutselen via een vervalst e-mailbericht of een valse website, geeft meestal zijn volledige e-mailadres op, terwijl de gegevens die publiek werden gemaakt de 'rauwe' Belgacomgebruikersnamen waren: generische cijfer- en lettercombinaties die beginnen met de letters 'fa'. Dat betekent wellicht dat al die duizenden gegevens werden gelekt uit de systemen van Belgacom zelf. Dat kan via een hackingaanval zijn gebeurd, maar dan zou Belgacom dat wel hebben ontdekt. Misschien komen de gegevens van iemand die in het bedrijf werkt?"

Volgens Margot kunnen de accountgegevens van een Belgacomklant, indien die in verkeerde handen zouden vallen, voor weinig doeleinden worden gebruikt: alleen e-mails sturen en de gebruikersgegevens veranderen, maar ze kunnen bijvoorbeeld niet worden ingezet om toegang te krijgen tot de webbankinggegevens van de klant. Willems onderschrijft dat. "Maar het feit dat je aan de e-mails van een klant kunt, vind ik toch wel ernstig. Zo kunnen buitgemaakte adressen worden gebruikt om spam te versturen."


Hacker chanteert Belgacom na 'kraken van internetmodems'