Festival in de zorg

Digitalisering in onze maatschappij - Part II

Robert Weedage & Wendy Knigge

POLITIE

Data is overal, ook dat van u?!

✓Apparaten lekken informatie

✓Social media

✓Databases (gelekt)

✓Onbewust openbaar

✓Verlies van laptop/usb

Data is geld waard.

Toekomst zal zich meer richten op gepersonaliseerde digitale criminaliteit.

Wat komt er op ons af ?

NOS NIEUWS • BINNENLAND • TECH • DI 25 JUNI, 16:36

KPN: 112-storing mogelijk door software-fout

hackers?

Vitale infrastructuur wordt steeds vaker gehackt. Tot nu toe zonde gevolgen. Maar: 'Het kan elk moment overal vandaan komen.'

DE STENTOR ZATERDAG 10 OKTOBER 2015 REGIO 9

• 15-jarige Robin uit Ruurlo is leider van groepje hackers

Stel pubers legt provider Ziggo plat

Blackfury is zijn alter ego op internet, zijn leeftijd is 15. De politie houdt hem mede verantwoordelijk voor meerdere DDoS- aanvallen.

door **Lucien Baard**
RUURLO

De hackersgroep Anon Nazi legde afgelopen zomer het internet van Ziggo dagen plat. Geen zware jongens, maar voornamelijk pubers. Zoals de twee Achterhoekers Robin W. uit Ruurlo (15) en de 14-jarige Diederik de Z. uit Lochem. Alias Blackfury en Foxelvox.

De politie hield na maanden onderzoek dinsdag de vijf jongeren van 14 tot 21 jaar aan vanwege meerdere grote DDoS-aanvallen op internetprovider Ziggo. Door die aanval kwamen 1,8 miljoen klanten zonder internet en e-mail te zitten, onder wie een groot aantal uit deze regio. In anoniem geposte Youtube-filmpjes werd Ziggo destijds ook bedreigd met nieuwe aanslagen, als het bedrijf zijn service niet zou verbeteren. Met uitzondering van de oudste verdachte zijn de hackers allemaal weer vrij. Ze komen uit Den Helder, Schoorl, Vinkeveen, Lochem en 'de gemeente Berkelland', maakte de politie bekend. Ze zouden elkaar in het dagelijks leven niet kennen, maar alleen via contacten op het internet. Ruurloër Robin W. - die schuil zou gaan onder Blackfury - wordt door experts en andere hackers, betiteld als de leider. Diederik de Z. – alias Foxelvox, wordt omschreven als toch minimaal nummer twee in de hiërarchie van de groep Anon Nazi. Diederik had eerder op Youtube een filmpje gepost waarin hij zelf laat doorschemeren bij de aanval betrokken te zijn geweest. Hij en zijn ouders zijn niet voor commentaar bereikbaar. De moeder van Robin wel, maar zij zegt dat het helemaal nog niet vaststaat dat haar zoon werkelijk betrokken is bij de aanval op Ziggo.

„Het is niet verstandig om er nu wat over te zeggen. Er wordt wel beweerd dat mijn zoon 'Blackfury' is, maar er wordt wel meer onwaarheid gesproken." Maar anderen in het wereldje weten het wel zeker. Internet-expert bij Redsocs, zelf voormalig hacker, Rickey Gevers, had de groep al op de korrel: „Er zijn sterke signalen dat die Blackfury inderdaad de servers beheerde waarmee de aanval werd uitgevoerd. Daarmee zou je hem kunnen zien als de leider."

Aanzien

Rickey Gevers volgde de groep beroepsmatig, zegt hij, maar had de Ziggo-aanval niet verwacht. „Ze waren tot dan alleen bezig met klein spul. Fora en discussieplatforms van spelletjes platleggen, dat werk. Maar ineens hebben ze besloten om een grote als Ziggo te pakken. Geen idee waarom. Misschien om te laten zien hoe goed ze zijn."

De vijf jongens kozen bewust voor de groepsnaam Anon Nazi. Dat zou een verwijzing zijn naar de eerdere roemruchte hackersgroep UG Nazi uit 2011. Die werd wereldnieuws door Amerikaanse overheidssites te hacken en gegevens van de FBI en CIA maar ook Twitteraccounts van beroemdheden op straat te gooien. De leider Cosmo the God was toen ook 15 jaar; hij verdween in een jeugdgevangenis in Californië. 'Ug' stond voor Undergrond. In het geval van de Ziggo-aanval staat Anon voor Anoniem. Waar nazi op slaat is onduidelijk: het gaat niet om neo-nazi's.

Snel na de aanvallen gingen al wat namen rond. Foxelvox, Blackonix, Sector_NL. Voormalig hacker en internetexpert Rickey Gevers lukte het om Ruurloër Blackfury aan de groep te linken, nadat op een hackerforum Hackflag 'een kennis' zijn mond voorbij praatte. 'Ik heb hun op Skype. Ze zijn gestopt met het groep, de Owner is helemaal bang AKA BlackFury. Hij is en gesmeerd, nu nog wachten of hij ze veraad.'

Gevers: „O stoer om te lat mensen van zo meestal wachte worden. Uiteins tijd wel uit wie val zit. Alleen g teraan als een a krijgt, zoals bij men kwamen v een andere hac ceerde: 'Boeffi'.

Script kiddi

Er ontstond Ziggo-aanval deze Boeffi en ceerde hun ge ten dat ze de beste h de attack op Ziggo g wou ze laten zien da op internet. Ik vond ver gaan; een stelletj gevolgen zien van h geringschattend 'scr gebruik van techniek zijn ontwikkeld; scr vaak weinig verstan

Maar kinderspel en Ziggo is het 'erns tie zal hen zeker ver schade verhaalt is or provider wil niet zeg de is.

ilmpje: Hackers stelen BMW 6 binnen 3 minuten

Pokémon GO: 'Advocaat gemeente lijkt kansrijk in zaak overlast Kijkduin'

Foto: Richard Mulder

stelen dankzij enkele bugs in de beveiliging van de nieuwe chips die in de sleutels zitten.

RTL Nederland betaalt hackers 8500 euro na ransomwareaanval

RTL Nederland heeft 8500 euro aan cybercrimi van een ransomewareaanval. De systemen kon middel van back-ups, maar er is besloten om d

RTL Nieuws meldt dat het is ingegaan op de eis va bitcoin te betalen aan de criminelen achter de aanv systemen kon herstellen met back-ups. Volgens R

'Garmin heeft ransomware-losgeld betaald'

Garmin lijkt betaald te hebben voor de decryptor van de WastedLocker-ransomware waardoor het vorige maand getroffen werd. BleepingComputer heeft deze decryptor in handen weten te krijgen en aangezien er geen bekende kwetsbaarheid in het algoritme zit, is er waarschijnlijk betaald.

BleepingComputer heeft een softwarepakketje in handen gekregen dat afkomstig zou zijn van de it-afdeling van Garmin. Daarin zit de decryptor en een aantal security-toepassingen. In die eerste zitten verwijzingen naar de bedrijven Emsisoft en Coveware, respectievelijk een cybersecuritybedrijf dat decryptors maakt op basis van decryption-keys en een ransomware-onderhandelaar. Emsisoft zegt nooit betrokken te zijn bij onderhandelingen en Coveware weigert commentaar.

Hoeveel Garmin betaald heeft, weet BleepingComputer niet zeker. Wel heeft het van een werknemer vernomen dat de gijzelnemers tien miljoen dollar aan losgeld eisten.

'Slachtoffers Almelo-hack staan compleet machteloos'

Gemeente Lochem door het oog van de naald bij hack

Het Staring College in de Gelderse plaatsen Lochem en Borculo heeft losgeld betaald aan hackers die de school in hun greep hadden.

Gemeente Hof van Twente platgelegd door hacker

De Veiligheidsregio Noord- en Oost-Gelderland (VNOG) is zaterdag getroffen door een aanval met ransomware. Hierdoor is het gebruik van het interne systeem beperkt en kan e-mail niet gebruikt worden.

Verdachten hacken school Apeldoorn opgepakt

Impact ?

Nieuws

Ransomwaregroep publiceert gigabytes aan gevoelige data gemeente Buren

donderdag 21 april 2022, 11:22 door **Redactie**, 18 **reacties**
Laatst bijgewerkt: 21-04-2022, 13:44

Een ransomwaregroep heeft onlangs weten in te breken op systemen van de gemeentes Buren en Neder-Betuwe, waarbij minstens honderddertig gigabyte aan data is buitgemaakt en op internet gepubliceerd. Volgens de gemeente Buren blijkt uit de eerste inventarisatie dat het ook om gevoelige persoonsgegevens en vertrouwelijke informatie gaat. Een volledig beeld van de gestolen en gepubliceerde data, het gaat om ruim 730.000 bestanden, wordt uiterlijk begin volgende week verwacht.

"We weten nu dat er inderdaad persoonlijke gegevens gestolen zijn en dat vinden we heel erg. We zetten man en macht in om te achterhalen om wat voor gegevens het precies gaat en van wie. We lopen alle bestanden na", **zegt** burgemeester Josan Meijers. "Zo weten we van wie er belangrijke gegevens, zoals identiteitsgegevens, zijn gelekt. Inwoners en medewerkers van wie persoonlijke of vertrouwelijke gegevens zijn buit gemaakt, informeren wij zodra bekend is om welke gegevens het gaat."

Volgens de gemeente heeft de aanval en het datalek geen gevolgen voor de dienstverlening richting inwoners. Wel zegt de gemeente alert te zijn op signalen dat gegevens door anderen worden gebruikt. "Als blijkt dat er persoonlijke en vertrouwelijke gegevens van inwoners en medewerkers zijn buit gemaakt, nemen wij contact op met de betreffende personen." Hoe de aanval precies kon plaatsvinden laat de gemeente niet weten. Zodra er meer informatie bekend is komt de gemeente met een update.

Update

De aanvallers claimen **vijf terabyte** aan data van beide gemeentes te hebben buitgemaakt, waarvan ze nu 130 gigabyte hebben gepubliceerd.

Oost In samenwerking met **RTV Oost**

NOS Nieuws • Dinsdag 16 maart 2021, 13:58

Hack bij gemeente Hof van Twente veroorzaakt door te simpel wachtwoord

Een fout van de systeembeheerder heeft ervoor gezorgd dat hackers eind vorig jaar vrij spel hadden in de computersystemen van de gemeente Hof van Twente. Dat blijkt uit onderzoek van een cybersecuritybedrijf.

Impact ?

EXCLUSIEF

Illegale handel in privégegevens miljoenen Nederlanders uit coronasystemen GGD

25 januari 2021 15:50
Aangepast: 13 september 2021 15:46

Een medewerker van het bron- en contactonderzoek bij de GGD.

Werkwijze infecties / risico’s

• Social engineering	• Criminelen bereiden steeds beter voor welk bedrijf ze aanvallen.
• Phishing	• Doelgericht infecteren met passende communicatie: factuurfraude
• Kwetsbaarheid	• Veel netwerken bevatten nog een kwetsbaarheid in software / modems / wachtwoorden
• Gebruiker	• Zolang we gebruikers houden …..
• Dienst ICT	• Wie monitort wie ?

Keuzes / ontdekking / incident response

- Back-up
- Schade
- Onderhandelen
- Wie doet onderzoek
- Protocol
- Wie bepaalt ?

Back-up :

[illegible]

- Hoe is de back-up georganiseerd. Er zijn veel bedrijven die betalen voor een back-up oplossing maar niet exact weten hoe [illegible]
- Wat is de schade op korte / lange termijn.
- [illegible] 'opnieuw beginnen' een optie.
- Kans op opsporen of identificatie van [illegible]
- [illegible] integrale afstemming met andere activiteiten organisatie
- Back-up terugzetten of sporen bewaren ?
- Afstemming Politie
- Assistentie politie ?
- Data gebackupt of enkel ontoegankelijk?
- Wie maakt de uiteindelijke beslissing ?
- In welke mate zijn back-ups getest en ingeregeld

Advies

✓Hoe en waar is eigen data in beheer

✓Wie beveiligt de infrastructuur / data

✓Protocol bij een hack, scenario’s

✓ICT als sluitpost – onderdeel van de begroting

✓Meldplicht Data Lekken

Het kan ons allemaal overkomen...

POLITIE