Storing bij Defensie toont aan: zonder cybersecurity staat Nederland stil

Posted on 31 augustus 2024 by Bart Collard

De Nederlandse overheidsdiensten kampten deze week met een grote technische storing. Vliegverkeer van en naar Eindhoven Airport, dat onder beheer van Defensie valt, was niet mogelijk. Meerdere gemeenten konden geen rijbewijzen en paspoorten afgeven. Ambtenaren van diverse ministeries hadden problemen met inloggen. Ook de systemen in de Tweede Kamer werken niet naar behoren. De storing kwam door een softwarefout op een van de IT-netwerken van Defensie, meldde minister Ruben Brekelmans in een Kamerbrief.

De vraag die bij een opvallend lange storing rijst, is natuurlijk of het hier ging om een cyberaanval, zoals die in het verleden plaatsvonden vanuit landen als China, Rusland en Iran. Defensie ontkende dit in een persbericht, maar tegenover *NRC* was het ministerie iets genuanceerder: 'tot dusver' lijkt het niet te gaan om sabotage maar er is nog geen 'volledige duidelijkheid'.

Lopend kwetsbaarheidsonderzoek

Het probleem in deze casus zou zitten in het Netherlands Armed Forces Integrated Network (NAFIN). 'Deze kabel,' zo valt te lezen op de website van de Algemene Rekenkamer, 'is het product van een publiek-private samenwerking tussen Defensie en onder meer KPN. Dit "gesloten" glasvezelnetwerk is zo'n 3.300 kilometer lang en is noodzakelijk voor vitale overheidstaken. Het verbindt niet alleen zo'n 180 defensielocaties met elkaar, maar ook 70 locaties die niet van Defensie zijn. Dit zijn onder meer de ministeries en hun datacenters, politielocaties, het centrale deel van het C2000-netwerk waarmee de hulpdiensten communiceren, maar ook enkele NAVO-hoofdkwartieren en de koppeling met de militaire netwerken van België en Duitsland.'

Kritische infrastructuur dus voor Nederland geldt, maar ook voor de NAVO. Vermeldenswaard is dat de Algemene Rekenkamer daarom sinds november 2023 bezig is te onderzoeken 'hoe de minister van Defensie ervoor zorgt dat het NAFIN weerbaar is tegen zowel fysieke als digitale cyberaanvallen'. Ook wordt onderzoek gedaan naar de detectiemogelijkheden van cyberaanvallen – het is immers niet altijd duidelijk dat het om een aanval gaat – en hoe daarop wordt gereageerd: welke protocollen liggen er klaar als er niet meer op de systemen kan worden vertrouwd en in hoeverre zijn die protocollen bekend en werkbaar?

Technologische ontwikkelingen kunnen het leven veiliger en makkelijker maken, maar die ontwikkelingen gaan nu sneller dan ooit tevoren. Het is daarom essentieel om kritisch na te denken over hun betekenis, om normatieve vragen te stellen en om de data-ethische kant te belichten. Zoals ik in Het Recht op Misinformatie schrijf, is het belangrijk om niet blindelings mee te gaan in narratieven over het 'aanpakken' van bijvoorbeeld misinformatie. Want wat betekent het om op internet berichten te verwijderen? En zou het medicijn niet erger kunnen zijn dan de kwaal?

Systemen waarin politie- of GGD-medewerkers gezamenlijk het verloop van een melding kunnen verwerken, zijn ontzettend handig. Er kan dan effectiever en efficiënter worden gewerkt. Maar wat als het systeem er plots mee stopt? Weten de medewerkers dan wat ze moeten doen? De reeds aangevraagde rijbewijzen van burgers zijn al geprint en liggen klaar in de gemeentehuizen, maar de verwerking van de afgifte kan in het systeem niet plaatsvinden. Een systeemprobleem wordt zo ook een bureaucratisch probleem. De overkoepelende vraag is: zijn we niet te

afhankelijk geworden van bepaalde technologieën? Kunnen we nog functioneren zonder die hulpmiddelen?

Wat als banksaldo's worden gewist?

Dit soort vragen geven ook te denken over andere ontwikkelingen. Er zijn initiateven als een Europese id-wallet en een digitale euro; we doen nu onze meeste geldzaken al digitaal en veel mensen hebben geen significante hoeveelheden contant geld meer in huis. Maar wat als burgers door een storing geen toegang meer hebben tot hun rekening? Of nog erger: wat als banksaldo's op een of andere manier worden gewist?

Uit de storing bij Defensie moet lering worden getrokken, of het nu ging om een cyberaanval of om een pijnlijke menselijke fout. De casus toont de kwetsbaarheid van het systeem aan en de afhankelijkheid van technologie voor allerlei vitale processen in onze samenleving. Het belang van cybersecurity kan nauwelijks worden overschat.

*Van **Bart Collard** verscheen in 2023 'Het recht op misinformatie'. Het boek is overal te koop en te bestellen, ook in de winkel van Wynia's Week. Kijk **HIER**.*

*De donateurs maken **Wynia's Week** mogelijk. Doet u mee? Doneren kan op verschillende manieren. Kijk **HIER**. Hartelijk dank!*