CYBERDREIGINGSBEELD 2015

SECTOR ONDERWIJS EN ONDERZOEK

TLP WHITE

Bart Bosma, SURFnet
bart.bosma@surfnet.nl

Type Dreiging	Manifestatie van dreiging		Relevantie (kans x impact)		
Type Dreiging	Gebeurtenis		Onderwijs	Onderzoek	Bedrijfsvoering
1. Verkrijging en openbaarmaking van data	• Onderzoeksgegevens worden gestolen • Privacygevoelige informatie wordt gelekt en gepubliceerd • Blauwdruk van opstelling onderzoeksinstellingen komt in verkeerde handen • Fraude door verkrijgen van data over toetsen en opgaven	→	MIDDEN	HOOG	MIDDEN
2.Identiteitsfraude	• Student laat iemand anders examen maken • Student doet zich voor als andere student of medewerker om inzage te krijgen in tentamens • Activist doet zich voor als onderzoeker • Student doet zich voor als medewerker en manipuleert studieresultaten	→	HOOG	MIDDEN	LAAG
3. Verstoring ICT	• DDoS-aanval legt IT-infrastructuur plat • Kritieke onderzoeksdata of examendata worden vernietigd • Opzet van onderzoeksinstellingen wordt gesaboteerd • Onderwijsmiddelen worden onbruikbaar door malware (bijvoorbeeld eLearning of het netwerk)	↑	MIDDEN	MIDDEN	MIDDEN
4. Manipulatie van digitaal opgeslagen data	• Studieresultaten worden vervalst • Manipulatie van onderzoeksgegevens • Aanpassing van bedrijfsvoering data	↓	HOOG	LAAG	LAAG
5. Spionage	• Onderzoeksgegevens worden afgetapt • Via een derde partij wordt intellectueel eigendom gestolen • Controleren van buitenlandse studenten door staten	→	LAAG	HOOG	LAAG
6. Overname en misbruik ICT	• Opstelling van onderzoeksinstellingen overgenomen • Systemen of accounts worden misbruikt voor andere doeleinden (botnet, mining, spam)	→	LAAG	MIDDEN	MIDDEN
7. Bewust beschadigen imago	• Website wordt beklad • Social media account wordt gehackt	→	LAAG	LAAG	LAAG

Impact van de dreiging t.o.v. 2014: ↓ = afgenomen, → = gelijk gebleven, ↑ = toegenomen

Dreigingen sector onderwijs en onderzoek

LAAG	MIDDEN	HOOG
"Er zijn geen nieuwe trends of fenomenen waar de dreiging van uitgaat.	"Er zijn nieuwe trends en fenomenen waargenomen waar de dreiging van uitgaat.	"Er zijn duidelijke ontwikkelingen die de dreiging opportuun maken.

SURF

CYBERDREIGINGSBEELD 2015

Published (in Dutch) on December 4, 2015

www.surf.nl/cyberdreigingsbeeld

Top threats that that were identified:

- Data leakage
- Identity fraud
- ICT disturbance
- Espionage

Cases

4.2 Ransomware

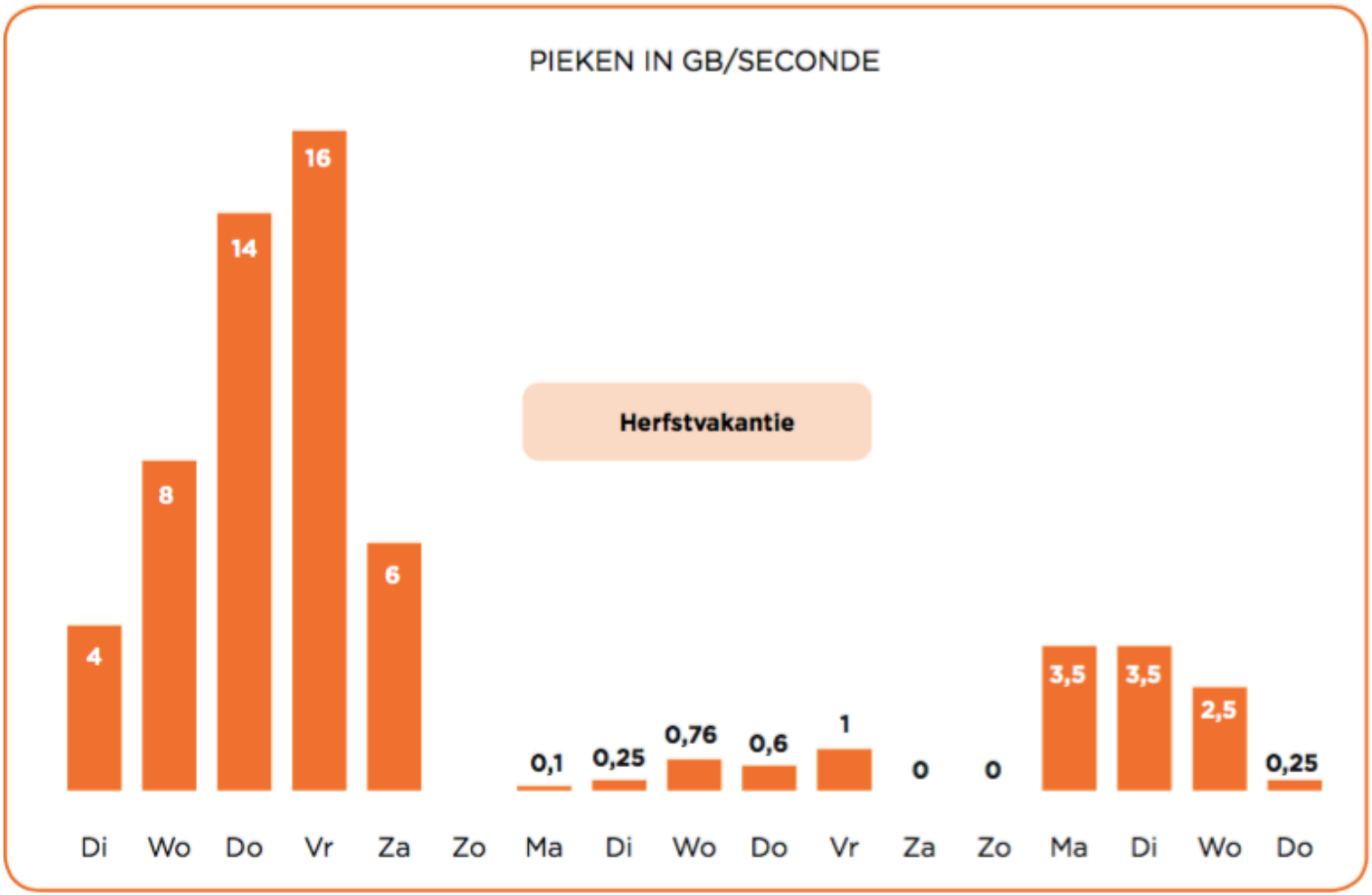
4.2.1 Het incident

Begin 2015 werd de Vrije Universiteit Amsterdam getro en door CryptoLocker, een vorm van ransomware (zie kader op pagina 29). In eerste instantie leek de malware binnengekomen te zijn via e-mail van buiten, maar al snel bleek dat de malware muteerde en zich kennelijk ook aan e-mailberichten van interne gebruikers wist te koppelen. Uiteindelijk zijn zo'n 200 computers besmet geraakt.

Kostenraming CryptoLocker-incident

werkzaamheden	tijd/incident	aantal	tijd in uren
aanmelding probleem	5 min.	200	16,67
diagnose probleem	10 min.	200	33,33
bepalen kortetermijnoplossing			2,00
bepalen langetermijnoplossing			8,00
inregelen oplossing			4,00
herstel besmette systemen	1 uur	200	200,00
terugzetten van data	3 uur	200	600,00
verloren werktijd + herstel verloren data	8 uur	200	1600,00
aanpassing procedures			
		Totaal uren	2464,00
		Totaal dagen	308
		Kosten per dag	€500,00
		Totaal kosten	€154.000,00

Cases



Toename van aanvalsactiviteit voor, tijdens en na de herfstvakantie 2015 (bron: SURFcert)

Cases

SPIONAGE: BRITSE GEHEIME DIENST BESPIONEERDE JARENLANG BELGACOM-KLANTEN

Bij de digitale aanval op Belgacom kon de Britse geheime dienst veel meer communicatie onderscheppen dan tot nu toe werd aangenomen. De geheime dienst GCHQ raakte in 2011 binnen in het netwerk door drie werknemers te hacken. Daarna kon de GCHQ twee en een half jaar lang ongestoord rondsnuffelen in het netwerk van Belgacom en dochterbedrijf BICS. De geheime dienst kon zo de communicatie onderscheppen van de individuele klanten van Belgacom zelf, van de NAVO en de EU, en van de klanten van honderden internationale telecomproviders.

(De Standaard, 13 december 2014)

CYBERDREIGINGSBEELD 2015