Visiting address
Turfmarkt 147
2511 DP The Hague

Postal address
PO Box 20011
2500 EA The Hague

I www.cybersecurityraad.nl
T +31 (0)70 751 5333 (secretariat)
E info@cybersecurityraad.nl

Ministry of Justice and Security
Attn Prof. F.B.J. Grapperhaus, LLM
PO Box 20301
2500 EH The Hague

Date
11 September 2020

Subject
CSR Recommendation Letter concerning response to WRR report and Citrix evaluation

Your Excellency,

The Cyber Security Council (hereinafter referred to as the council) is issuing this recommendation in response to your *Letter to Parliament concerning the evaluation of Citrix-related problems and the government response to the WRR report entitled* '*Voorbereiden op digitale ontwrichting*' (*Preparing for digital disruption*), dated 20 March 2020. In that letter, you reflect on the findings in the report from the Netherlands Scientific Council for Government Policy (WRR) and what these mean as an expansion on, adjustment of or supplement to the policies of this government. You also refer to the lessons learned from the problems with Citrix, expound on what this government is doing to prepare for digital incidents and specify the measures being taken to increase this country's digital resilience.

The council has taken cognisance of the measures you suggest in connection with responding to digital incidents and crises with digital aspects, preventing such incidents from occurring and strengthening digital resilience. The council is of the opinion that your chosen approach represents a vital step in the right direction. In a number of areas, however, the council feels that your approach calls for a tightening and/or expansion of the measures to be taken. Thanks in part to the COVID-19 pandemic, we have been catapulted into a new phase of our digital society. In addition to paralysing our physical society for a lengthy period, the virus is now also obliging us to make even more intensive use of our digital infrastructure and all its associated facilities and resources. A large part of the Dutch population is currently working remotely, studying remotely and maintaining social contacts remotely. Data traffic has greatly increased in the recent period as well. Our dependence on digital technology and the providers of that technology has consequently undergone a considerable and structural increase – and along with it the digital scope for attack available for wilful misuse by malicious parties. Furthermore, the picture presented by the recently published Cyber Security Assessment Netherlands 2020 remains troubling. The digital resilience of our society is more vital, therefore, than ever. We must preserve our ability to take decisive action in response to wrongdoing and/or cyberattacks and must be able to rely on the security and continuity of our digital infrastructure, especially under the present circumstances but into the future as well. Effective measures must be taken to that end.

A mature system of information exchange must be realised as quickly as possible, and a cycle consisting of testing, evaluation and implementation of the resulting points for improvement must be established. Full efforts must also be maintained to further the interests of investigation and prosecution. To achieve these aims, the council considers it necessary to increase supervision of cooperation.[1]

[1] CSR Declaration of Urgency, Cyber Security Council, 31 March 2020

Nationwide exchange of information

The adage that an ounce of prevention is worth a pound of cure also applies in the digital domain. The council sees this reflected in real-world practice, where a great deal of attention is devoted to preventing incidents. These efforts hinge on the accurate, timely and comprehensible provision of information. Information about cybersecurity must be easily accessible to all organisations in the Netherlands and must provide realistic prospects for action. Despite previous recommendations[2] in this area from the council, parties including the Netherlands Scientific Council for Government Policy[3] and various ongoing initiatives, the council observes that, while attention is being focused on making threat-related information widely available through a nationwide network of information hubs (the *Landelijk Dekkend Stelsel* or LDS), the pace at which the system is being rolled out is insufficient to meet the growing demand for information that organisations need as a basis for measures aimed at increasing their digital resilience. The nationwide provision of information has emerged as a persistent hurdle. To a significant degree, this can be attributed to the fact that the nationwide network is still under construction, as you also indicated in your Letter to Parliament concerning the evaluation of Citrix-related problems and the government response to the WRR report and in your 'Policy response to CSAN 2020 and progress report on the NCSA'. In addition, as it stands now, to a certain extent the information exchange is discretionary in nature, as providing relevant information is not always mandatory. And in some cases, providing information is not possible under the prevailing legislation and regulations.

The council considers it both necessary and urgent that we accelerate the roll-out of the nationwide network and enhance the exchange of information between victims, the National Cyber Security Centre (NCSC), the Digital Trust Centre (DTC) and investigative bodies. The non-obligatory nature must be remedied and any statutory or other obstacles in this area must be eliminated. We simply cannot afford a situation in which the provision of information in the Netherlands falters or the country's digital resilience is threatened. The increasing momentum of the digital developments we are currently facing serves to further heighten the urgency.

Supervision of cooperation

Accelerating the roll-out of the nationwide network and improving the exchange of information will not suffice. As the WRR also concluded, we are unable to prevent all incidents; the Netherlands Scientific Council for Government Policy is in favour of better preparation for digital disruption by means including adequate powers to prevent escalation. The threat assessment laid out in the CSAN 2020 also underscores the importance of proper preparation for potential disruption. It is vital, therefore, that organisations be sufficiently resilient; they must be able to recover quickly from a crisis or from the harmful effects of cybercrime. In order to effectively combat cybercrime, it is important that investigative authorities be actively involved when such incidents occur. As previously observed in the National Plan for Digital Emergencies, the current situation entails a risk of conflict in this area, namely between the interests of an organisation – which strives to maintain business continuity – and the interests of the investigative authorities, which wish to secure data and detect and prosecute criminals (based on reports). The council wishes to underscore the Netherlands Scientific Council for Government Policy's fourth recommendation and attaches great value to an evaluation of the legal grounds as a means to establish clear roles and relationships between government bodies on the cybersecurity and investigation side.

[2] CSR Recommendation 2017, No. 2: 'Towards a nationwide system of information exchanges', advice on information sharing with regard to cybersecurity and cybercrime]
[3] Netherlands Scientific Council for Government Policy (2019) 'Preparing for digital disruption', WRR Report 101, The Hague, p. 55-60

In the council's opinion, the fact that these roles and relationships are not yet obvious is due in part to fragmentation as a result of a division of responsibilities and a limited mandate. For the NCSC, this was partly compensated during the COVID-19 pandemic by the recently adopted emergency legislation[4] that granted the NCSC mandate to provide assistance to hospitals, pharmaceutical suppliers, research centres and so on in the event of digital threats and incidents. The council is of the opinion that, in general, government and other parties should more frequently be brought together during incidents in order to adopt a joint approach when implementing the necessary actions and measures.

The council considers a pro-active approach to supervision of cooperation vital and emphatically recommends that government parties on the cybersecurity and investigation side be granted the necessary mandate and sufficient capabilities to take joint action in response to incidents. This will allow for streamlining of the advisory and support services provided to affected organisations, with proportionate attention paid to the interests of investigation and limiting the damage to society.

Focus on other improvements

In addition to the provision of correct and timely information before and during incidents and a proper balance between organisational interests and the interests of the government – including the interests of investigation – the council wishes to point out the valuable lessons that can be distilled from incidents, especially larger ones. This recommendation from the council therefore addresses the need to strengthen the processes and mechanisms that go into effect *after* a (potentially major) digital incident has taken place. As a supplement to the measures suggested in your letter, the council recommends thorough evaluation of incidents with major impact on vital processes as *standard* and implementing the resulting lessons learned and improvements. With this in mind, the council is pleased with the rapid evaluation of the main points of the Citrix problem and the recent announcement that the Dutch Safety Board will conduct a more in-depth exploration of the impact of this incident. The council strongly urges ensuring that the lessons learned from these evaluations actually have been, or will be, implemented. However, the council also notes that in-depth evaluation of incidents is not yet the standard course of action at this time, nor is the implementation of improvements. There is currently no uniform method available for the evaluation of incidents at multiple levels, and the results of such evaluations are not always shared with all involved parties. Organisations also frequently fail to report incidents, which is not conducive to developing an effective approach to fighting cybercrime. Improvement in this area will likewise contribute to enhancing the digital resilience of organisations.

Like the Netherlands Scientific Council for Government Policy, the council is of the opinion that conducting exercises is crucial in order to increase digital preparedness. While this applies to all organisations, it is particularly true for the critical national infrastructure, where the failure of digital systems can quickly lead to social disruption. The government and private sectors of vital importance must be able to consult quickly, and the respective roles and actions must be clear to all parties. This calls for a high degree of proficiency. The Citrix incident has made it clear that this proficiency has not yet been attained.
Although you indicate in your response to the CSAN 2020 that cyber exercises are increasingly becoming the norm, the council considers it necessary to establish a structural programme of exercises in which the government and private sectors of vital importance conduct frequent joint drills involving digital outages. This cannot and must not be limited to a single exercise such as Isidoor III. It is essential that this programme incorporate the major points for improvement from previously conducted evaluations.

[4] Parliamentary Paper 26643, No. 695: Policy response to CSAN 2020 and progress report on the NCSA, 29 June 2020, pages 2-3

Recommendations

The council makes the following recommendations:

1. Ensure acceleration of the roll-out of the nationwide network of information hubs (the LDS) and the improvement of the information provision, so that, by the end of 2021, all organisations in the Netherlands have access to the information they need in order to achieve digital resilience. Eliminate any statutory or other obstacles.
2. Within one year, ensure that the government authorities on the cybersecurity and detection side are granted sufficient mandate, capabilities and supervision of coordination to enable them – during larger incidents – to coordinate their advice and act in a way that balances attention for the continuity of organisations, the interest of investigation and the goal of limiting the damage to society.
3. Within two years' time, develop and implement a cycle of (potentially annual) public-private cyber exercises, evaluations of major incidents and implementation of points for improvement. This cycle must be geared to the learning ability of organisations and should contribute to strengthening the digital resilience of our society. Crucial points for improvement identified during previous in-depth evaluations and the conclusions and recommendations in research reports from parties such as the Netherlands Court of Audit, advisory councils and/or supervisory bodies must be taken into account as well.

In order to achieve the aforementioned aims, not only will supervision of coordination be vital, but mutual trust as well, along with an open attitude among the parties involved. This open mindset must focus on strengthening digital resilience not only within the organisation but throughout the entire chain(s), thereby also reinforcing our digital society and social safety.

These measures, among other activities, can help us improve the handling of digital and other incidents in the Netherlands while also increasing the resilience of affected organisations and facilitating cooperation between public and private parties aimed at strengthening our country's digital resilience.

In this way, we can work towards an open, secure and prosperous digital Netherlands.

On behalf of the Cyber Security Council,

Hans de Jong
CSR co-chair