Open Letter

Switch to the Cloud, think before you start

Recently, the media has written extensively about the ransomware attacks on municipalities, universities, colleges and the NWO. In addition to these well-known ransomware attacks, we also see a lot attacks on Microsoft Exchange mail servers, in which new errors are found all the time. It turns out that this many email systems can be hacked, and system administrators have their hands full with it fix errors in the Microsoft software. Fortunately, Microsoft's cloud-based email systems (Office 365), and those of the other big tech companies are relatively safe. It therefore seems only understandable that there to outsource e-mail and other services to the apparently secure Cloud solutions of the American Big Tech Industry.

University boards also increasingly decide to outsource the maintenance of ICT services to US Cloud Giants. That is special, because in the Volkskrant of December 2019, the rectors of the Dutch universities on the contrary “to draw a line” in order to reduce the dependence on American to reduce tech companies. Apparently long-term strategic thinking loses to short-term operational problems. But is that wise, and will the bill of a failing strategic action be on us? not break the deadline? Before irreversible decisions are made, there are a number of points to consider: administrators and university councils should first consider.

Privacy and security
It is important for students to find a safe learning environment, where there is room to make mistakes and to learn from this. It must be impossible for students' privacy-sensitive data to be misused for other purposes is becoming. However, commercial companies that offer a Cloud solution can use data for multiple purposes use. For example, bearing in mind the Cambridge Analytica scandal, we must note that the security and privacy protection of our students at commercial Cloud providers is not always guaranteed.

Politics
By transferring the data of employees and students of Dutch universities to American Cloud providers, we do not only place that data outside the European territory, but also within the 'walled gardens' of these Cloud providers, which are subject to US laws and regulations. But not only the data, but even the we outsource authorization to services. We thereby elevate the Facebooks, Googles, Amazons and Microsofts of this world not only as a manager of our data, but also as a border police for that data. When the NSA formulates a legal basis, it may well be that the US government gains access to the e-mail traffic and the data of students and employees at Dutch universities. Take as an analogy the physical access to our country: should we pass border control at Schiphol and the issuance of passports to a outsource to a foreign nation?

Foreign students
In recent years we have had to observe that the American government can force companies and organizations to to cooperate with American political wishes. This raises questions regarding the data of foreign students and staff from countries with which geopolitical tensions exist, for example from China or Iran. Is Is it conceivable that an American government would force us to ban students from certain countries? Have Iranian Do students who work at home from their mother country still have access to Office 365 in this time of Corona? we find that acceptable?

Legal
In 2016, the EU and the US signed the “Privacy Shield” treaty, protecting the privacy of European citizens should be guaranteed. But last summer, judges of the European Court decided that this too treaty does not comply with European privacy legislation. There is therefore a real chance that Dutch judges forbid universities to store data in the US Cloud any longer. With a view to Given this legal uncertainty, it therefore seems unwise to migrate to a US cloud now.

Financial
In the short term, it can indeed be advantageous to outsource ICT services to the Cloud. But does one also have calculated what the migration costs are if we ever want to get rid of it, for example because the judge has ordered us to do so forces? What are the long-term costs and do we still have the experts with an understanding of the matter? Do we have a clear picture of this?

Ethics
Is it justifiable if a company fails to deliver secure e-mail software, then reward it by completely dependent on that company and outsource all your e-mail and ICT services to that company?

Understandably, the recent ransomware and the Exchange mail attacks for some universities (extra) arguments for outsourcing the management of crucial ICT services. Cybersecurity is an ever-growing problem, and keeping one's own infrastructure safe and secure is becoming increasingly difficult. But why is the e-mail infrastructure and other services (including authorization) no longer work together with universities of applied sciences, UMCs, MBOs and other institutions dedicated to SURF, the organization of and for us? Although outsourcing to SURF on can be more difficult in the short term than outsourcing to the (American) Big Tech companies, in the somewhat longer many problems can be avoided in the long run.

We, the Dutch cybersecurity scientists who have united within the Academic Cyber Security Society (ACCSS) [1] , call on university boards and councils to develop a strategic vision, before fait accomplis are created. Don't forget that for the Big Tech companies: “you can check-in” anytime you like, but you can never leave”.

Prof. dr. dr. ir. Aiko Pras - professor of internet security (UT)
Prof. dr. Dr Andreas Peter - adjunct professor of data security (UT)
Prof. dr. mr. Arno Lodder - professor of Internet law (VU)
Prof. dr. Dr Bart Jacobs - Professor of Security, Privacy and Identity (RUN)
Prof. dr. dr. Bert-Jaap Koops - professor of technology regulation (Tilburg University)
Prof. dr. dr. Bibi van den Berg - professor of Cybersecurity Governance (Leiden University)
Prof. dr. ir. Cees de Laat - professor of System and Network Engineering (UvA)
Prof. dr. dr. Frederik Zuiderveen Borgesius - professor of ICT and law (RUN)
Prof. dr. ir. Herbert Bos - professor of Systems and Network Security (VU)
Prof. dr. dr. Joris van Hoboken - associate professor information law (UvA) and professor (VUB)
Prof. dr. dr. Jeanne Mifsud Bonnici - professor of European Technology and Human Rights (RUG)
Prof. dr. mr. Lokke Moerel - professor of Global ICT Law (Tilburg University)
dr. Marleen Weulen Kranenbarg - Assistant Professor of Criminology (VU)
Prof. dr. dr. Marten van Dijk - group leader Computer Security (CWI)
Prof. dr. dr. Michel van Eeten - professor of governance of cybersecurity (TUD)
Prof. dr. ir. Roland M. van Rijswijk-Deij - adjunct professor of network security (UT)
Prof. dr. dr. Ronald Leenes - professor of Regulating Socio-Technical Change (TILT)
Prof. dr. dr. Stijn Ruiter - professor of social & behavioral sciences (UU), senior researcher (NSCR)
Prof. dr. dr. Tanja Lange - professor of Coding Theory and Cryptology (TU/e)

Questions, comments about this open letter can be sent to: info@accss.nl

[1] www.accss.nl