VREDE EN RECHT

The Hague

Toward **cyber resilient** cities

Is your city prepared? The three cities met for elaborate discussions at the One Conference on October 2nd in The Hague. The cities of The Hague, Atlanta and Greater Manchester shared best practices and lessons learned on how to prevent, respond to and recover from a cyberattack that impacts the city.

PIONEERED BY THE ROCKEFELLER FOUNDATION

100 RESILIENT CITIES

Imagine all of the data and computers in your City Hall being out of service due to a cyberattack. Or a cyber security breach in one of the companies within your city that eventually leads to hazards for public safety. Is your city prepared? Are you aware of the vulnerabilities in your municipality? And do you know who to call when the heat is on? On Monday October 1st and Tuesday October 2nd 2018, the municipalities of Atlanta, The Hague and Greater Manchester met to bring together city resilience planning and cyber security agendas.

Being partners within the 100 Resilient Cities network, the cities of The Hague, Atlanta and Greater Manchester wanted to share best practices and lessons learned on how to prevent, respond to and recover from a cyberattack that impacts the city. What can and should a city do? Who is responsible for what? And how can a city prepare itself for a cyber crisis?

The three cities met for elaborate discussions on Monday October 1st, and convened in a panel at the One Conference of the Dutch National Cyber Security Center on October 2nd in The Hague. During this international conference, the Resilient The Hague team hosted a side-event named ‘Cities under Cyber Attack’ in a packed room. During the side-event three cities from the 100 Resilient Cities network came together to share their experiences on cyber-resilience: Ria Aiken, Director Emergency Preparedness at the city of Atlanta, Kathryn Oldham CRO of Greater Manchester and Jeroen Schipper, Chief Information Security Officer of The Hague.

On both days, the discussions centered around a case presented by Ria Aiken, Director Emergency Preparedness at the city of Atlanta. On March 22nd 2018 she got called out of bed with the message that the city was facing a cyberattack (see box): A significant number of devices connected to a particular city network had been infected and a majority of the data on those devices was encrypted. The city had just begun a process of migrating their on-premise servers into the cloud, email being one of them, and critical infrastructure facilities including the emergency center (911), the airport, and the water treatment facilities were on their own separate networks, they were minimally impacted by the ransomware attack. But still, most of the municipality’s everyday customer facing platforms faced major problems, and some of them even had to be shut down for a longer period of time.

During the meetings, a myriad of topics came to the table. In this article we present the main themes that were discussed and share the lessons learned.

1. Governance

When the cyberattack hit Atlanta, the Mayor had been in office for a little over two months. The COO had been on the job for for 4 days, and an Interim CIO had been named three weeks prior to the ransomware attack. Luckily for Atlanta, the city had been preparing for a major event, and only three weeks earlier had met with the Department of Homeland Security Cyber Security Advisor and a member of the FBI to discuss available programs to assist the city. When the ransomware attack occurred, they called federal representatives from DHS, FBI, and Secret Service who were more than willing to help. Another fortunate circumstance was that the city had just signed a cyber security insurance policy, which provided them with a list of preselected vendors they could call who could help them through the response, restoration, and recovery efforts. 'But since we had no prior engagements with these companies, we had to interview a number of them within a few days to be ensure that we selected the best firm given the nature of the incident and the situation we were in,' Aiken says.

LESSONS LEARNED

During the discussions, governance, business continuity, and cross-functional and cross-sector planning turned out to be three of the main factors cities can and should optimize in order to prepare for and respond to cyber emergencies.
That means not only that you need to know who within your municipality is in charge and accountable for cyber resilience, but also which internal and external parties should be involved and in what way. Perhaps more importantly, a city should ensure that on a holistic level its governance and performance review board structures are working effectively so that a whole-system approach is taken to embedding cyber resilience.
Cities should also be aware of their own resource constraints. What expertise does the designated cyber incidence response team have, and what is lacking? Who can you call in to help? Make sure you have established relationships with federal and industrial partners before something happens, and invest time in maintaining these relationships.
Finally, whether a city has insurance, is thinking of securing insurance, or doesn't have insurance, they are encouraged to proactively review a list of providers and conduct pre-screenings with potential providers before an incident occurs.

The Hague
Promote inclusion to improve digital resilience

In addition to the physical city, digital cities are starting to emerge. This increasing amount of digitization comes with new opportunities to deliver services faster, easier, and more tailor-made to the needs of the inhabitants. But digitization also comes with risks. Not only of cyberattacks, but also of excluding those citizens, enterprises or small municipalities that cannot keep pace with the fast developments in the digital world. These groups could be left behind when it comes to digital resilience.

The City of The Hague tries to tackle this issue on different levels. In City Hall itself, cyber security is firmly rooted on an operational, tactical and strategic level. Five of the primary departments have internal information security officers who report to the Chief Information Security Officer. He has an advisory role on the strategic level, for example in procurement. This way the city is able to develop and implement a municipality-wide cyber security strategy.

Furthermore, The Hague has started developing a 'trainee like' network to share knowledge and experiences with smaller municipalities in the vicinity. Talented young people are attracted to become public servants, by offering them a program in which they can gain experience in various roles and with different responsibilities in a variety of municipalities, ultimately training them to become CISO's of larger cities. When working in the smaller towns, they will effectively act as the local CISO. This enables them to gain experience in taking responsibility and having direct contact with the Mayor about policy issues.

Finally, but no less important: The Hague invests on different levels in raising awareness of cyber security. The city deploys awareness campaigns for its own employees, for example by developing a privacy game called 'Gegevensweg', organizes special public events like Hackathons, in which ethical hackers are invited to hack the city, and co-organizes the yearly cyber security week.

2. Know your assets and vulnerabilities

The problem is that we are often working in silo's' is a phrase that was commonly used during the meetings. Often different municipal departments have their own way of working and use their own applications to run their daily business. To be able to respond swiftly and appropriately to a cyber threat, you need to know on a city level how many applications you have within your infrastructure, which of those are critical for your operations and how they are interconnected and interdependent. Furthermore, when you know where your vulnerabilities are, you know where to put an extra lock on the cyber door.

LESSONS LEARNED

Proper asset management and procurement are crucial to get a grip on what applications are running, who is maintaining them, what the associated security risks are and when they should or could be phased out. Too often departments or even individuals are able to install new applications onto the network, without any control mechanisms in place to mitigate the associated risks. Security should be included in the procurement process, all the way up to board level. This also goes for involving third parties or subcontractors to provide some of the city's services. Ensuring that the appropriate IT professionals are included in developing the appropriate IT related language for procurement terms and conditions is a key first step to ensuring vendors are adhering up to your security standards.

For example, in Greater Manchester it was during the midst of a major crisis when a subcontractor brought in by a third party was shown to have little knowledge of the crucial role their service had in providing family members with information about the whereabouts of their loved ones. And that the servers the subcontractor was responsible for should have had the capacity needed to enable police services from all over the country to help take calls from the public.

As a result of the ransomware attack, Atlanta is in the process of installing a cross-functional infrastructure investment committee, in which the CTO, CIO, and CISO together with the key department representatives evaluate every new application and the applicability, interdependencies and vulnerabilities before they decide if the 'project' and corresponding application is approved to move forward.

Atlanta
The SamSam ransomware attack

When the cyberattack hit Atlanta, the Mayor had been in office for a little over two months. The COO had been on the job for for 4 days, and an Interim CIO had been named three weeks prior to the ransomware attack. Luckily for Atlanta, the city had been preparing for a major event, and only three weeks earlier had met with the Department of Homeland Security Cyber Security Advisor and a member of the FBI to discuss available programs to assist the city. When the ransomware attack occurred, they called federal representatives from DHS, FBI, and Secret Service who were more than willing to help. Another fortunate circumstance was that the city had just signed a cyber security insurance policy, which provided them with a list of preselected vendors they could call who could help them through the response, restoration, and recovery efforts. 'But since we had no prior engagements with these companies, we had to interview a number of them within a few days to be ensure that we selected the best firm given the nature of the incident and the situation we were in,' Aiken says.

3. Information and communication

Providing and collecting information is key in all three phases of a cyber crisis: in the prevention, the restoration and the recovery phases. During the Atlanta attack, the incident response team organized up to four briefings a day to keep the employees, leadership, and organizations involved up to date. They also held numerous press conferences and established an external website to provide up-to-date information for the public about the services that were and weren't affected, and where they could go to pay their bills or ask questions.

Furthermore, since municipalities are spending public money, it is imperative that you are transparent about the costs involved in responding to a cyber emergency and the corresponding restoration and recovery efforts. Implementing a real-time cost capture and burn rate program is essential to understanding the associated costs resulting from an incident. Weekly discussions with vendors to work through potential project related questions (goods, services, and labor) can reduce the amount of discrepancies when final invoices are submitted.

LESSONS LEARNED

As goes for every crisis, communication is key. But in the case of a cyber crisis, this aspect needs extra attention, since many of the automated internal processes could cease to work when your network is down. Start by making an inventory of who needs to get what information in what format at what time, and come up with well-documented, organized processes to keep everybody up-to-date, both inside and outside of your organization.

Be opportunistic and always learn from a crisis. It's only during a crisis that you can get a real overview of the consequences for daily activities. And after the crisis is over, people tend to forget many of the things that went wrong. With this in mind, the city of Atlanta conducted interviews with a number of department employees during the crisis and discussed how it impacted their operations, and to confirm what manual processes were and weren't in place. Reverting to manual operations turned out to be a massive operation, since the city had to trace back the paper trails to see who had to fill out which forms, and where to send them next.

In the preparation phase, it is therefore wise to determine which services are crucial, and map out and describe the manual alternative for them.

Greater Manchester Area
Multi-agency planning

What makes a cyber threat so different from any other threat, such as terrorism or a natural disaster? The results are often the same: loss of important services, people lacking access to their homes, healthcare demands and so on. First of all, in case of a cyber crisis, there is no notion of geography, an infection crosses all borders. Secondly, the pace at which things can move is unprecedented. Third, a cyberattack can be multi seated having impact in multiple places.

Therefore, to mitigate a cyberattack, multi-agency planning is crucial. Public-private partnerships should be at the heart of such planning. Furthermore, within the municipality, emergence response teams and IT-professionals should be brought together and should learn to speak the same language. Because in case of an attack, they will need to cooperate to respond to the attack, while maintaining business continuity. Simply shutting off all services is no option, since that may influence the response possibilities in a negative way.

Greater Manchester is developing several initiatives to bring these different parties together. It has established a Cyber Foundry that connects four universities and the GMCA (Greater Manchester Combined Authority) to create a trusted environment for doing business digitally, make SMEs more resilient in the cyber domain, and use academic cyber research as a technology accelerator for local SME's. The city's Greater Manchester Resilience Unit is also participating in the cross-sector Greater Manchester Cyber Advisory Group and partnering with the ThinkLab at the University of Salford. Finally, the municipality takes an active role in promoting cyber security measures with citizens and businesses.

4. Interdependencies and cascading effects

Cyber incidents tend to not come alone. Take the incident that occurred on September 23rd 2018 in Amsterdam. One of the large Dutch telecom providers experienced a glitch in their network. This influenced the radiophones of the local public transport system, as a result of which, buses, subways and trams could not be used for a few hours.

Another example occurred in June 2017, when the container terminal of the Danish shipping company Møller-Mærsk in the Rotterdam harbor was hit by a cyberattack. Since the containers could not be loaded, a growing row of trucks congested the roads in Rotterdam.

Gaining insight into interdependencies and possible cascading effects is not easy. Even in the ideal world, where every application is carefully assessed by the information department before it is deployed, sometimes a single line in software that becomes corrupted might lead to unexpected effects with a series of consequences happening at the same time and yet being apparently unconnected. Still, it helps to do an exercise, and think through how different systems are linked with each other, and what would happen if one of these systems unexpectedly malfunctions, either due to a cyberattack or due to other causes.

Simulations, war games or involving ethical hackers might help to gain insight into where the vulnerabilities are and to identify unexpected chains of events which might occur due to an error in one of the individual applications.

5. Unresolved questions

Though the two-day meeting definitively accelerated the learning process when it comes to making cities cyber resilient, multiple issues still need to be addressed in order to be able to mitigate and manage cyber risks. Here we pose some of the questions that are still wide open and invite you to join us in deliberating on the best way forward. Since cyber security could be regarded as the new natural hazard, let's come together to build a global practice of cyber resilience among governments, NGOs, the private sector and individual citizens.

- What role can municipalities play to prevent, respond to and recover from a digital crisis, and what is the role of businesses and other organizations in ensuring business continuity?
- To what extent is a city responsible for creating cyber security awareness or protecting its citizens in their home environment?
- When an emergency in the physical city happens, the municipality's responsibilities are clear. Where does the responsibility for a major cyber incident, occurring in the virtual world, lie within the city?
- What special mandate does or should a municipality have when a cyber incident occurs within its city?
- Who defines which systems or applications are critical? And how do you make the distinction between critical and important?
- What is the next step in making cities digitally resilient as we all welcome technology into our lives?

For more information:

www.100resilientcities.org
www.resilientthehague.nl
resilience@denhaag.nl
@resilienthague