International Center for Enterprise Preparedness (INTERCEP)

Lessons Learned From Cyber Attacks On City Governments

Web Forum

On April 30, 2018 Jake Williams, Founder and President of Rendition Infosec and SANS Instructor and Course Author led a web forum on Lessons Learned from City Government Cyber Attacks. Cyber-attacks on city governments, including the recent ransomware attack on Atlanta, pose a threat to both the public and private sectors. Below is a summary of the web forum.

Introduction

What do we see on attacks on city governments/municipalities? There have been several incidents of both data theft and multiple types of ransomware.

Ransomware attacks may be of different types. In a typical commodity ransomware scenario, for example, an attachment from an email results in the encryption of a machine. This is limited to a computer and there is no lateral movement.

Advanced ransomware attacks can be more damaging since they have the potential to move throughout networks, with automated lateral movement. With this type of attack it is possible to enter a network, move through the network, remove backups, and then turn on the ransomware.

Supply chain attacks may come from vendors and others that are part of an organization’s supply chain and that have access to your environment. The NotPetya ransomware attack is an example of this since it used a specific software used by many organizations.

Many municipalities are not taking action to better protect themselves against ransomware attacks. In some cases municipalities may mistakenly think that they are not at risk because there are more important targets than them, and that this protects them somehow. In other cases it may be because they have nothing in their budget to act proactively. This leads to a mentality of “we’ll address these problems next year when we have a budget for it.”

In some cases municipalities fail to adopt protection measures because they may not be aware of regulations that may apply to them. An example is the General Data Protection Regulation (GDPR) which applies to citizens of the European Union (EU) that may be living in a U.S. municipality. Failure to address IT security and data protection issues may result in liability.

IT security is getting harder not easier. Attackers benefit from the lessons of previous attacks and they are getting more sophisticated. They also have the advantage of asymmetric warfare. An organization has to be right all the time to avoid begin hacked whereas the attackers only have to get it right once.
The targets are also shifting. Attackers have honed their skills targeting financial institutions and retail, and as those become harder targets, they are moving to other targets they can benefit from, including targets they may not have considered before. This includes municipalities. In some cases attackers can take advantage of unusual situations to maximize the pressure they put on their targets. It could be a municipality that is hosting a major international event for example.

**Ransomware versus Data Theft**

What are attackers really targeting? Sometimes it’s difficult to tell because it is easy to drown in a sea of security data. The things an attacker may be interested in include confidentiality, integrity of data, and availability of a system. In the case of the recent attack on Atlanta it was an attack on the availability of their system as well as an integrity of data attack.

What controls do we have to protect data? Oftentimes people misrepresent things when they say they are protected from attacks. Decision-makers do not need to be cyber professionals but they should be cyber literate. When communicating with decision-makers and senior management about the need to include IT security in the budget it may be helpful to use analogies to things they are familiar with. This does not mean dumbing things down, it means presenting an accurate picture of the risk in ways that can be understood.

The main takeaway point in terms of management is that an organization should have a ransomware plan.

The impacts of a ransomware attack can be severe, whether it is a commodity ransomware or an advanced ransomware or a targeted ransomware attack. This is particularly true if the attacker activates the ransomware after they have deleted backups.

How can an organization deal with the impacts? It is critical to have war-gamed all potential scenarios and to be prepared in terms of the response.

With municipalities, it’s important to know if a municipality can legally pay the ransom. Does their charter support that? It would imply funding a criminal activity which could be illegal.

Another important consideration is that if a municipality pays they could be subsequently targeted again since the attacker would then think that the municipality or whoever they targeted would pay again.

How often does the same group come back and probe activity? It could be 3-6 months. In cases of targeted ransomware there is sometimes evidence that the attackers have left doors behind to access a system.

When a ransom is paid the organization affected gets their data back. Sometimes if they are unable to decrypt the files for some reason, they will refund the targeted organization because they want to establish the process as being credible.
Does the city charter allow a municipality to pay an extortion fee? If not, why would an attacker target a municipality? It could be that an attacker knows they will not get paid but they know such an attack would get a lot of attention in the media/press, which would make it likely another target would pay.

In some cases a ransomware attack may be part of an automated system of advanced ransomware, and they may not care if they don’t get paid, and will just keep looking for vulnerable targets.

**Critical Safety Systems**

Humans do not make good decisions under stress. It is important for a municipality or any organization to have discussions about how to respond to an incident before an attack happens instead of having these discussions while something is happening.

If an organization already has a good disaster recovery planning effort, this topic may have been covered already.

Ransomware is not always ransomware – sometimes an attacker may use ransomware to cover their tracks after they have done data theft. It can wipe forensic evidence/artifacts. When you see a ransomware attack an organization should consider whether it could be covering up other activity on their network. This could also be the case when you have an insider threat where someone has walked off with some data, and as news begins to spread of the data theft a ransomware emerges.

The importance of network monitoring cannot be overstated. If an organization does not see any data infiltration it doesn’t mean there wasn’t any. It is critical to have real time security monitoring. Legislation is shifting back to “prove that it didn’t happen”. If you can’t prove it didn’t happen, then it probably did happen. Network monitoring is a critical part of this process.

**General Data Protection Regulation (GDPR)**

Many municipalities may think the General Data Protection Regulation (GDPR) does not apply to them. But it may apply to municipalities because they may have EU citizens who are on the municipal water and sewer services and this regulation may apply to how the municipality is using that data. As GDPR kicks in a municipality may be liable for that. How does this regulation play into a cyber-attack? It relates to reporting requirements because they are more stringent than any other regulation.

A municipality should also determine how “right to be forgotten” laws may conflict with records retention laws for public organizations.

A municipality may lose a lot of records of payments as a result of ransomware, and they may not know who or how many of their customers are EU citizens.
**Unfunded Mandates**

For most municipalities ransomware protection and response is an unfunded mandate, and they may think that they will get a budget after an incident. But this is too late. Nobody wants to be the next city affected by ransomware. How would it look on the front page of a major newspaper after it has been reported?

What should a municipality budget for? Enterprise back-up systems that are rotated offline are critical. Security monitoring is also an absolute must.

Incident response retainers, including gap assessments and table tops are also important. Most municipalities have contingency plans in place for incidents such as a natural disaster. They have pre-negotiated arrangements with contractors to provide additional generators, construction equipment, etc. Having pre-negotiated contracts with contractors to assist in the case of a cyber-attack is just as important.

Identifying risk is absolutely critical. What are you seeing that maybe we haven’t seen yet? Hearing about what attackers have done and looking for sources of unknown risk should be part of the monitoring effort.

This is not a “do it yourself” endeavor. Municipalities and IT managers can’t work alone.

Network monitoring is critical to prove whether data infiltration did or did not happen. Without that you are just guessing about what happened.

How reliable is network monitoring? Are they able to cover their tracks? Nothing is 100% reliable, they can cover their tracks but there is usually some evidence. We can see some of the communication, they have left some bread crumbs.

**Takeaway points**

- Ransomware isn’t always ransomware, it may be used to cover for another type of attack such as data theft.
- General Data Protection Regulation (GDPR) may apply to municipalities – consult your general counsel to find out for sure.
- Any given municipality or organization will probably get hit by ransomware at some point so this is something that should be planned for.
- Municipalities should budget for ransomware protection and response.
Additional Resources:

- Rendition InfoSec: [https://www.renditioninfosec.com/](https://www.renditioninfosec.com/)