Ransomware attacks on cities are rising

August 28 2019, by David Wall

Credit: Jimmy Liao from Pexels

A ransomware campaign that targeted 23 US cities across Texas has raised serious concerns about the vulnerability of local governments and public services to cyber-attacks. These events come not long after

similar attacks on governmental and business organizations in Indiana, Florida and elsewhere. They reflect a general shift in ransomware tactics from "spray and pray" attacks on large numbers of individual consumers, to "big game hunting," which targets organizations, usually through people in positions of power.

A recent report from cyber-security firm Malwarebytes found a 363% increase in ransomware detections against businesses and organizations (as opposed to individuals) from 2018 to 2019. Put simply, cyber-criminals see an opportunity to extort far more money from organizations than individuals. Although the majority of ransomware attacks were found to occur in the US, local governments around the world are equally vulnerable.

Ransomware usually spreads via phishing emails or links to infected websites, relying on human error to gain access to systems. As its name suggests, ransomware is designed to block access to data, systems or services until a ransom is paid. At a technical level, cities tend to be fairly easy targets because they often have bespoke operating systems, with parts that are old and out-of-date, as well as ineffective back-up measures.

Cities also tend to lack system-wide security policies, so if cyber-criminals gain entry through one system, they can then access others and wreak havoc by freezing essential data and preventing the delivery of services. But even if organizations have improved their technical security, my research with my colleague Lena Connolly has found that few put equal emphasis on training employees to identify and resist attacks.

Target acquired

Employees in many small and medium-sized organizations, like local

governments, often do not recognize their organization's true commercial value to criminals, and commonly think they are unlikely to be targeted. As a result, they might also develop bad habits—such as using work systems for personal reasons—which can increase vulnerability.

Offenders will do their homework before launching an attack, in order to create the most severe disruption they possibly can. After all, the greater the pressure to pay the ransom, the higher they can set the tariff.

Attackers identify key individuals to target and seek out vulnerabilities such as computers which have been left switched on outside of working hours, or have not been updated. Once they've worked out who to target, cyber-criminals deploy "social engineering" techniques, such as phishing, which psychologically manipulate victims into opening an email attachment or clicking on a link, which allows the ransomware program into the organization's operating system.

Credit: Unsplash/CC0 Public Domain

To pay or not to pay?

Whether or not to pay the ransom is not a straightforward decision for city authorities with vital public services on the line. Most policing agencies instruct victims not to pay, but as Mayor Stephen Witt of Lake City, Florida, put it after his ward was targeted: "With your heart, you really don't want to pay these guys. But, dollars and cents, representing the citizens, that was the right thing to do."

Another problem is that ransomware is not always deployed to extort money—so paying the ransom doesn't guarantee that data will be

restored. Attackers can have varying motives, skills and resources—working out their motive (often with very little information) is therefore crucial.

Rather than simply making money using ransomware, some cyber-criminals might seek to disable market competitors who provide competing goods or services. Or, they may use the attacks for political gain, to reduce public confidence in a local government's ability to deliver essential services. In such cases, the data is unlikely ever to be restored, even if the ransom is paid.

Seeking cover

Many cities are insured against attacks, and insurers often pay the ransom to retrieve stolen data – sometimes employing third party negotiators, against national advice. Ironically, the knowledge that cyber-criminals are likely to get paid justifies the time they spend researching their target's weaknesses, and leaves the door open for repeat attacks. This was one of the reasons why cyber-criminals changed tactics and started targeting organizations in the first place.

This leaves city authorities a difficult choice, between paying to restore essential data and services (and encouraging cybercriminals) or admitting their systems have been compromised and facing up to social and political backlash. Even so, there are some measures city authorities can take to protect themselves, and their citizens, from ransomware.

Today, authorities need to assume that it's a matter of when—not if—an attack will happen. They should install back up systems for protected data that have the capacity to replace infected operating systems and databases if need be. For example, in the UK, research found that 27% of local government organizations were targets of ransomware in 2017. Yet 70% of their 430 respondents had backup systems in place, in

preparation for the EU's General Data Protection Regulation (GDPR), and could therefore recover from a ransomware attack much faster than their counterparts in the US.

Local authorities need to separate their data systems where possible and install appropriate levels of security. They also need to train employees about the nature of the threat and the impacts of their own actions when working within the organization's systems. They should also be aware of international schemes to prevent and mitigate ransomware (such as nomoreransom.org) – which provide advice and publish the keys to some ransomware online.

Public organizations must be able to think quickly and adapt to these new security threats—especially since cyber-criminals are always coming up with new techniques. Local governments need to be prepared to simultaneously prevent cyber-attacks, mitigate their effects when they do happen and bring cyber-criminals to justice.

Provided by The Conversation