EFFECTS OF CYBER ACTIVISM ON MUNICIPAL OPERATIONS

Ferguson Case Study, Lessons Learned

by William R. Powell Jr., Ph.D.

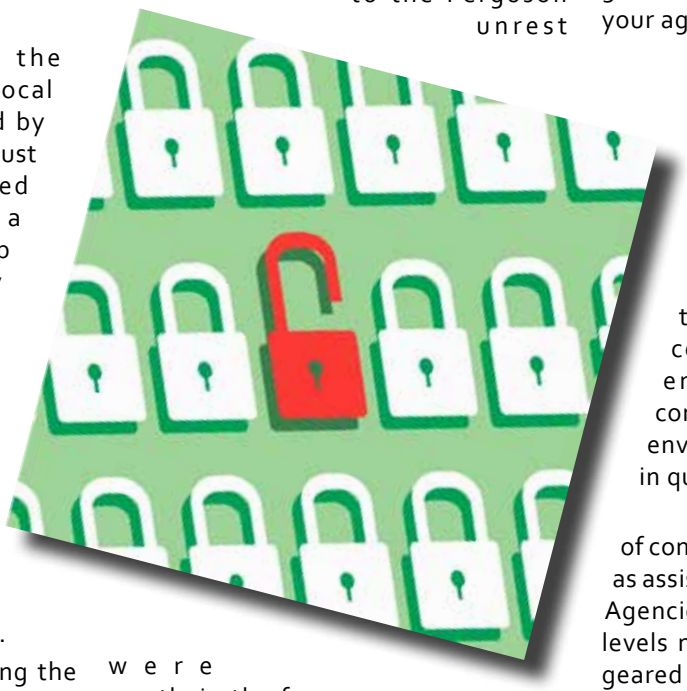
As many in the public arena know, we are constantly under scrutiny as to how we function and how we react to various situations. The Ferguson situation in August 2014 highlighted the need for municipal preparedness against cyberattacks on networks. This article describes items to consider to protect your municipality in the future.

Only three days after the Ferguson incident occurred, local municipalities were threatened by the group called "Anonymous;" just one day later they commenced their attack. Anonymous is a type of pseudo hacking group that participates in an activity called hacktivism. According to Wikipedia, hacktivism is, "the subversive use of computers and computer networks to promote a political agenda." There are many ways to cause this electronic mischief, including site defacement, site redirects, denial-of-service attacks, and information theft, among others.

- **Site Defacement**: Changing the appearance of a site or webpage
- **Site Redirects**: Moving a visitor to a webpage other than the one they requested
- **Information Theft**: Obtaining personal or financial information of another person
- **Denial of Service:** Depriving a resource of services they would normally have, such as email, network connectivity, etc.

Because of today's reliance on computers and access to the outside world through the Internet, hacktivism has become an effective tool in making a political statement. If connectivity is interrupted even briefly, it can have direct, adverse effect on an agency's ability to conduct business. By disrupting access to computer software and websites, hacktivists are essentially voicing their public opinion.

The attacks related to the Ferguson unrest were mostly in the form of distributed denial of services (DDoS) that entailed having a large number of computers spread across the globe continuously target the municipal websites to bring them down. The affected agencies' Internet connections and/or servers would become so overwhelmed with the massive amount of traffic that they could not process valid traffic. Since the attacks were spread across a large footprint, it was impossible to determine the initiator to stop the attack. It was not designed to gain access to any systems.



Preparedness is the key to minimize the effect of future attacks. Gathering information during the heat of battle is both cumbersome and time consuming. For many of us, it is not feasible to have every protection in place for every risk; but, having a plan in place for common, modern day threats is an achievable goal. Consider creating a plan to ready your agency for a hacktivist's attack.

The Plan

Your plan should contain the following elements:

Inventory: Start with a complete inventory of your Internet presence, including things like IP addresses, vendor contacts, domain registration, email configuration and the construction of any cloud operating environment. This will greatly help in quickly dealing with an attack.

Points of Contact: Include a list of contacts for both notification as well as assistance in dealing with the attack. Agencies at both the state and federal levels may have cyber groups that are geared to assist you in these areas. It is best to know what help is available before you need it.

Risk Analysis: Conduct a risk analysis of your services outside of your network to determine what Internet-facing services are critical and what services could be temporarily shut down. This is an important planning step as it may be necessary to turn off some services in order to ensure the critical services can operate.

Public Press Releases: Turning services off could also negatively impact your constituents' perceptions of your agency should something occur. Plan

now for how to deal with the unforeseen outages, including public press releases. Include what to share and what not to share about what is affected, and what you are doing to resolve it. It is best to be very vague concerning your protections and actions.

Remediation: Remediation is the term used to reduce the effects of a DDoS attack against your network. Before you experience a DDoS attack, ask your Internet service provider (ISP) if they offer any DDoS remediation service and the associated costs that you should expect. If the ISP does not provide DDoS remediation, several commercial vendors provide the service. Review their solutions and pricing models prior to needing their services. Negotiate for their service now rather than when you are under attack, as you may have fewer options if you wait. Remediation can be very costly depending on the vendor and the type of service they provide.

Incident Response Plan: Document all of the items contained in the plan and assign each task to a responsible party. This will save time when it is needed the most.

Identifying An Attack

Initially an attack will most likely appear as an Internet service outage affecting your Internet availability, email traffic, VPN, or some other aspect of your services. If this occurs, a call to your ISP will help determine the cause and effect.

In the event of a DDoS attack, work quickly with your ISP or remediation vendor to regain control and protect other aspects of your network environment. Keep in mind that a DDoS attack may be designed to initially avert your attention away from other forms of hacking that sometimes are possible as a result of the weaknesses that were exploited during the DDoS attack itself. Therefore, do not rush to bring services back online too quickly. It may be beneficial to only bring services back up online once a thorough security screening is conducted. Depending on the threat and your preparedness to handle it, it may be necessary to remove the Internet connection to your firewall to prevent harmful traffic from gaining access to your services.

REJIS

Regional Justice Information Service

Connecting People and Information

Services:

- Municipal Court Case Management
- Regional Law Enforcement Information Sharing Service
- Automated Policy Acknowledgement System
- ID Card Creation and Printing

REJIS is a government agency that specializes in meeting the technology needs of our government partners since 1974!

www.rejis.org 314-535-1950

Summary

None of us wish to be in the position of having to deal with situations similar to what took place in Ferguson in 2014, but as part of your preparedness for such an event, it is important that you include the information technology aspect in your preparedness plans. Plan now by creating an inventory list and a list of contacts; conducting a risk analysis; developing public press releases; researching remediation services; and creating an incident response strategy. Although creating such a plan will not provide protection from such an event, it will position your municipality to better handle the crisis and allow staff to focus on areas where they are needed most.❑

Dr. Powell is the general manager of the Regional Justice Information Service (REJIS) supporting public sector government agencies within Missouri, Illinois, and Kansas. In this role, Powell provides strategic leadership of all information technology support activities for more than 300 governmental agencies. Find more information at www.regis.org.

Learn more about cyber activism from REGIS at the MML Annual Conference in September! Check for details in the conference program on page 17 of this issue.