Large City Strengthens Resiliency by Adopting Zero Trust Microsegmentation Principles

INDUSTRY:
Municipalities

HEADQUARTERS:
U.S.A.

Overview

One of the largest metropolitan areas in the United States at over 7.5 million people has over 40 different departments through which it provides a wide variety of services to its residents. As a modern metropolis, commercial and cultural hub, remaining secure, and keeping legacy systems protected and current are the most prevalent concerns against the ever growing impatient and clever threat actors. The City experienced a major ransomware attack that impacted city services taking several weeks to restore and a painstaking comprehensive review of each individual system and device to ensure they were free of malware.

The malicious actors were able to gain access through one department and due to the over 40 different departments being structured laterally, once they had access to one, they had easy access to all, wreaking havoc quickly.

The Challenge

LEGACY SYSTEMS: The City was utilizing many legacy systems which were no longer supported by Microsoft, nor could they be updated, leaving them vulnerable to attacks. When the City looked into updating to a more modern system, they found it would be too costly.

FLAT NETWORK: The City had a completely flat network across over 40 departments. In other words, if a hacker would gain entry into the network of any one department, it could laterally move anywhere and reach the network of other departments.

COMPLICATED NETWORK ARCHITECTURE: Over the years, many people worked on the City's network and created multiple sets of rules. Most of these people were no longer at the City so historic institution knowledge was lacking.

LIMITED RESOURCES: The city has a shortage of info sec staff who can help them implement advanced controls. They also had limitations on hiring new additional personnel, so they were looking for a solution that was easy to implement and manage.

The Approach

Crawl, Walk and Run: At the outset, ColorTokens and City officials decided to break the program in three phases: crawl, walk and run.

1. In the Crawl phase, ColorTokens acted as an extension to the City and spent a lot of time training City personnel. We agreed the first desired outcome would provide confidence to the City's larger team and then worked closely to deliver that outcome.

2. In the Walk phase, the City's team felt more confident and began taking the lead on several steps of the Microsegmentation journey. ColorTokens' team was always present to assist the City personnel, but the idea was to drive up the adoption by letting the City lead.

3. In the run phase, we handed over operations to the City and they have been able to run microsegment applications on their own with little to no guidance from ColorTokens. Our team is on standby, but majority of the work is being performed by the City personnel.

Results and Benefits

With the ransomware at bay and microsegmentation in place, the City has been able to substantially reduce its attack surface and limit the blast radius. By isolating their legacy infrastructure ensuring that it has limited network access, this significantly reduces future risks of attack. The City is now able to easily prove and show how they are securing and storing credit card information securely by being PCI compliant. With a segmented network, the City is no longer vulnerable to exposing themselves with one door left open and the rest is fair game, over their previous flat network. To top off the human side of the benefits, the existing staff were well trained and working to segment even more applications.

Conclusion

With ColorTokens by their side from start to finish, the City found the exact level of support, partnership, and leadership they needed at each step of the Crawl, Walk, Run process. Throughout overcoming the ransomware attack, the City found that our solutions and services far outweighed those of our competitors, of Illumio and Guardicore; the other two vendors in consideration during the City's initial evaluation. And lastly, with the ease of implementation that comes with ColorTokens' approach and solution, the City's personnel were able to adapt quickly and recommend us to their peers, ensuring that this type of attack doesn't happen to someone else.