Napoleon Bonaparte Hardening Lesson

Itschak Mugzach,
Director at SecuriTeam software.

Acre is an ancient city on the north Mediterranean cost of Israel. In the 18th century, the area was ruled by the ottoman empire. The city was walled

In 1799, after Invasion to Egypt, napoleon wanted to return to Paris through the Balkan. These areas were owned by the Ottoman empire. As a first step, he decided to reach Syria and to incite a Syrian rebellion against the Ottomans and may be threaten the British empire in India. At the beginning of the occupation campaign, the France forces was able to take Gaza and Jaffa. However, the siege of Jaffa ended with two days of massacre and rape. The lesson learned by the Ottoman will be later implemented in Acre.

On the twenty of March, the France army arrived to Acre and laid siege on the city. Acre was well walled from the land sides and as the France artillery send by ships from Egypt to Haifa, was captured by the British armada. Nevertheless, Napoleon estimate that he will capitalize the city in to weeks. The fact was, that the city troops was informed on the Jaffa event few days before and refused to surrender. The siege lasted six weeks and on the 8 of May, the France soldiers was able to breach the walls of the city of Acre. However, the forces were not able to penetrate the city, as the defenders built during the siege a second wall few meters from the city walls. The France soldiers were captured between the walls and at the end of the battle, they lost 2,000 of them.

This historical story deals with hardening. The Ottomans understood the city walls may fall, as actually happened and prepared for such possibility.

Now, the story is relevant to many mainframe clients. I hear a lot of tales such as “we have a firewall between the mainframe and the world”, or even better, “some of the data is already on the corporate network, so why should a penetrator try access the mainframe”. The answer is simple. The data may be copied to network servers; however, the processes are still left on the mainframe and they are business critical tasks.

Protecting access to the mainframe is an important part of the security belt, but the mainframe itself should be protected. The process is called hardening, exactly as the ottoman troops hardened their walls.

The next step is to perform an assessment (or Security Readiness Review) to ensure that the system is actually hardened. Many vendors, including IBM supplies best practices or recommended settings to better protect their systems and products. DISA, a unit in the United States Department of Defense (DoD) created a framework called STIG to protect software and hardware assets which is based on the vendor's recommended best practices. STIG is the only framework that deals with mainframe operating systems and products, and as such, become the de-facto standard for hardening and verification for mainframes.

The problem is that organizations are being threatened not only by insiders and individuals, but also but crime organizations, governments, and terrorists. Both they have interest in your assets, such as money and information, and, in case of homeland infrastructure, to shut down services. Those organizations are well funded and use automatic scanning and penetration tool to try breach into systems. As the threats are continuous and changing, exactly as your security, which is changing according to business changing requirements.

There is a huge difference between the frequency your interfaces to the world are attacked and the slow pace of performing SRRs. The result is that at most of time, the organization is not in compliance. Manual assessments are so slow, that even during the assessment important security controls are changing. This situation leads to the need to review security in a continuous manner. It is also, a requirement by regulations, and standards such as the European General Data protection Regulation (Article 32(d)). Not only that, the CYBERSECURITY framework offered by NIST dictate the requirement for continuous measure of security. NIST CYBERSECURITY framework was adopted by many national organizations around the world.

NIST, the American National Institute of Standards and Technology, recognized the need and created another framework called ISCM. Information Security Continuous Monitoring is a collection of tools and procedures to ensure that at any given time, your organization is aware and understand the potential attack surface that can be used against it.

Think of the Ottoman troops leader, Al-Jazzar. After execution of an SRR, the security readiness review, he understood that the current city hardening plans are not sufficient and need to be updated. As a result, they built a second wall to create a second security belt.

Some points to think of:

- The Ottomans had a single city to protect at any single point in time. How many z/os Lpars (Logical Partitions) do you have?
- Does your organization part of the homeland infrastructure? What will happen to your organization and society in case of a breach?
- Do you perform security assessments? Are they aimed to provide your regulator a proof, or your interest is to protect the organization and client's assets?
- Do you lay or your infrastructure personnel to perform security, or you want to be able to monitor security yourself?

If you are interested in real time monitoring of the all mainframe lpar's security issues, have a look at IronSphere. IronSphere is an ISCM product for mainframe OS such as z/os that is based on ISCM and STIG frameworks to perform real-time security readiness reviews in a contiguous and modern way.

You don't need to be a mainframe expert in order to monitor mainframe security if you use IronSphere, as the product offers dashboards and detailed reports using standard browser.

About the author.
Itschak is an experienced systems programmer and mainframe penetration tester. He is the founder and creator of IronSphere, an ISCM product for mainframe operating systems that is based on the STIG framework.