A mainframe, just like any other computing platform, need to be audited. I mean status audit, not event audit which is different and will be discussed in my next article. What is status audit? This is the process usually called security assessment or Security Readiness Review (SRR).

For some reasons such as regulation, lack for tools or experience, SRRs are performed by an external auditor(s). Qualification is great, but expensive and results partial SRRs or less frequent. I met with clients that haven't performed an SRR for five or more years. They probably believe that "what you don't know can't hurt you". I think that a better resentence is "it hurt you, but you don't know".

Why SRR are important, and why frequent assessments are required? Simply because the mainframe has changed and the risk landscape has been changed. Mainframe supports almost any modern language, hosting Unix as part of the operating system, and implement IP based communication. These components are widely known (as opposed to SNA, the old communication protocol) and introduce new risks such buffer overflow, that couldn't be used in native mainframe languages.

The cyber threat landscape from late night pizza eaters living at their mother house to terrorist organizations, hostile governments and crime organizations. They are well funded and much riskier. Most, if not all, mainframe centric organizations are part of every nation homeland infrastructure, the problem is not organizational but national.

The bottom line is that threats are created every day, large organizations are facing hundreds of thousands attacks that are usually stopped at the firewall. But this return us to the original question:

Are you audit your systems like an old, manual gear car, or like a Tesla model 3 self-driving car?

I looked at some offerings for mainframe assessment. In the best case, it takes a team of mainframe audit specialist two weeks to collect the information and much more to analyze and report. At that period of time, systems are changing according to business demands, new functions and software. The result is that the report you'll get few weeks later is accurate, but to the date data was collected.

Until mid 90, the US federal agencies demanded to perform an SRR once in three years. At that time, the national Institute for Standards and technology (NIST), recognized the change in risk landscape and created ISCM. Information Security Contiguous Monitoring (ISCM) was a revolutionary discipline to conduct SRRs. Instead of an annually, expensive and outdated security review, a continuous, almost real-time, assessment that allows awareness of risks as they occur.

The way to achieve up to date awareness is to automate the process of audit by programming the audit process. At end, most of the issues found within misconfigured component, and too permissive access lists. Running the checks in a cyclic way creates a base line security report, that is updated by capturing changes to security controls and re-schedule the checks.

So, what are YOU doing to protect your organization, nation and clients?

About the Author.

Itschak Mugzach is a director at SecuriTeam Software and the developer of IronSphere, an ISCM product for IBM z/os and other legacy operating systems.