It’s not about what you have done;

It’s about what you are planning to do.

I cannot count how many times I have heard “the weakest link” reference in my career within the security field, but it does make you stop and pause. I would like to apply it specifically to a z/OS development LPAR’s security not being as strong as its counterpart z/OS production LPAR.

A person out to gain information on a competitor will want to get in to the system, look around, and get out as fast as possible. They may already know what your organization does, but more important, is what you are planning on doing six months from now.

For example; plans to build the next generation of an airplane are not always stored in a full production z/OS environment. In fact, there are many incidents where the plans of a company’s future were found in test and development environments. This dates back to the early years of the internet when one auditor representing a Fortune 50 company stated that corporate research and development databases had been copied and sold to a competitor, costing the corporation millions of dollars in lost sales opportunities.[1] Additionally, companies often replicate production data in development systems, making them just as much of a target as a fully locked down production LPAR.

[1] INTELLIGENCE THREAT HANDBOOK

https://fas.org/irp/nsa/ioss/threat96/part05.htm

Yet, development LPAR's often remain non-inclusive when it comes to an Information Security Continuous Monitoring (ISCM) program as described by National Institute of Standards and Technology's (SP) 800 directive.

NIST (SP) 800

"Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, defines Information Security Continuous Monitoring (ISCM) as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions."

z/OS Game Over

Enter UserID: Zwhd55

Enter Password:
MH1LLIFWWAS!

Mary Had a Little Lamb Its
Fleece Was White As Snow!

The easiest way into a system is by guessing a password. All of the RACF security in the world is not going to help your organization if a developer has used a weak password. Over 8 positions, using a number and a special character may not be enough.

Someone coming into a z/OS development LPAR from an ill-protected client machine is not farfetched. Depending on the organization's z/OS RACF configuration, there may be the 3 strikes and you are out rule (three bad password attempts and your ID is suspended). So, for avoidance purposes, they attempt to fly under the radar by hitting some RACF ID's with two attempts of password guessing and simply get out of the LPAR for today. There's no rush and time is on their side. They will probably come back tomorrow to do the same, and the day after, and the day after that until they have succeeded in getting a valid password, or are detected.

Summary

It is very difficult to detect this kind of pattern of abuse without the use of a z/OS Security Information Event Monitoring (SIEM) Agent and SIEM software. The purpose of having a z/OS Agent for ISCM is to provide your organization with a holistic view of your security posture in protecting your Intellectual Property, as well as your production customer information. The

regulatory fines are the same for either the next generation of an aircraft (development) or who is buying your jelly-beans (production customer data). A security violation and the loss of valuable data from a development LPAR could be as costly, perhaps more, than a production LPAR. The importance of pro-actively monitoring development z/OS LPAR's for invalid password attempts, in real-time, using SIEM software, cannot be stressed enough.

How many companies use a z/OS SIEM agent to monitor password violations on their z/OS development LPAR's?

Not many, due to lack of financial and personnel resources.

Does yours?