PROTECTING PII ON THE MAINFRAME

Let's kick this off by taking a step back and asking the question, "Why implement cybersecurity?" Compliance? Yes. Regulation? Yes. Continuous operation? Yes. You get the idea, but the common factor among all of these is ensuring that the business continues to function and that its data is protected. A business function can have downtime, but as long as the data is protected, there is still a valid business function to resume. If a business loses its data, then it can quite literally cease to exist—and that is before the regulatory bodies have begun to impose fines and penalties. Let me conclude the last three sentences in a more concise manner: the root reason for cybersecurity is to protect the business' data. This blog post will cover what personally identifiable information (PII) is and the processes for discovering, protecting, and testing that business-sensitive data.

What is PII?

In terms of cybersecurity, data is often referred to as PII—information held by a company that could be used to identify an individual. PII is the focus of many cybersecurity strategies because its loss or mismanagement can draw steep financial penalties. The strategy is a little bit more complex than this, however. While security strategies should certainly focus on PII, any and all data that could lead to failure of a business operation should also be managed in the same manner.

Data discovery and classification

Now comes the fun part—implementation. This can be done manually, but it is quite timeconsuming and complex. The reality is, to be effective, automation is required. The typical steps for data discovery and classification are:

1. Define all data sources that need to be classified, such as:
   a. All datasets, cataloged and non-cataloged, on all volumes defined to the LPAR
   b. All UNIX filesystems
   c. Any databases: IBM® Db2®, IBM® IMS™, virtual storage access method (VSAM), SQLite, etc.
2. Work with the compliance team to define classification labels, such as:
   a. Public data
   b. Private data
   c. Internal data
   d. Confidential data
   e. Restricted data
3. Work with the compliance team to define filters that will automatically detect potential data types, such as a credit card number, and load them into your automation solution
4. The following steps will now become your normal, continuous process:
   a. Scan the system to find any unclassified data
   b. If the data matches a filter, auto-define that classification and send for approval; if no filter is matched, classify as unknown and send for manual review
   c. Periodically check a compliance sample to ensure the method is compliant with the set of controls

How to protect your data and validate the protection

The level of protection applied to data should be directly correlated to the classification. Using an external security manager (ESM) like IBM® RACF®, ACF2™, or Top Secret to protect the data makes a lot of sense as it can then be built into roles, identity access management, and the organization's privileged access solution. The ESM can also be further utilized to categorize data, with the use of level ranges , which can directly correlate to classifications (e.g., everything over 100 is restricted data). To validate the protections put in place, regular security assessments and penetration testing (pentesting) will find any vulnerabilities.

Test data

One of the failures often found by the BMC Mainframe Security Services pentest and assessment team is that sensitive data has been copied for testing. The solution to this issue is to obfuscate production data when it is used for testing. When we talk about obfuscating data, it is not as simple as using a cipher offset of 1 to change every a to b and 1 to a 2. The data must behave the same as live data (for example, phone numbers need to reflect the location of the original phone number and a postal code needs to reflect the same area) for testing to be successful. Since generating test data is a continual requirement, using a software solution is the most sensible solution as part of your development lifecycle.

Summary

Finding out where your sensitive, PII, and organization-critical data is located is a key part of your security approach and must become part of your organization’s everyday strategy. Not only is it best practice, it is also part of many compliance frameworks. Following a discover, classify, and protect lifecycle will continually improve your organization’s security posture. When this process approaches maturity, it will put the organization in a strong position to explore implementing pervasive encryption. Further processes that should be brought into scope include roles matched to classification, as well as certain classifications of data accessed through privileged access only.