Safeguards Technical Assistance Memorandum for Protecting Federal Tax Information (FTI) in Integrated Voice Response (IVR) Systems

Introduction

The IRS Office of Safeguards has observed a number of agencies using integrated voice response (IVR) systems to process and transmit federal tax information (FTI) to their external customers. IVRs present opportunities for agencies to provide a convenient method for customers to access account information, which may include FTI, through a public facing telephone interface. This method of providing FTI to customers opens a new avenue for accessing FTI, and potentially exposes the FTI to compromise of confidentiality. For this reason measures need to be taken to protect the FTI that is provided to customers through an IVR system.

An IVR is a technology that allows a computer to detect voice and dual-tone multi-frequency signaling keypad inputs to allow customers to access a database via a telephone keypad or by speech recognition, after which they can service their own inquiries by following the instructions. IVR systems can respond with pre-recorded or dynamically generated audio to further direct users on how to proceed. IVR technology does not require human interaction over the telephone as the user's interaction with the database is predetermined by what the IVR system will allow the user access to.

IVR systems are phishing targets through man-in-the-middle attacks, where the attacker has put themselves into the middle of the transaction between the customer and the IVR system. Additionally taxpayers who call the telephone lines are at risk of having their Personally Identifiable Information (PII) inadvertently overheard.

Whether currently in use or planned to be deployed, there are FTI safeguarding measures required by the IRS Office of Safeguards to be in place given the security vulnerabilities associated with providing data via an IVR system. This memo will provide the policy requirements for ensuing the confidentiality of FTI is maintained by agencies that provide access to customers through an IVR system.

Requirements for FTI used in an IVR System

To utilize an IVR system that provides FTI over the telephone to a customer, the agency must meet the following requirements:

1. The local area network (LAN) segment where the IVR system resides is firewalled to prevent direct access from the Internet to the IVR system.
2. The operating system and associated software for each system within the architecture that receives, processes, stores or transmits FTI to an external customer through the IVR is hardened in accordance with the requirements of Publication 1075 and is subject to frequent vulnerability testing.
3. The agency must conduct an annual assessment of the security controls in place on all information systems used for receiving, processing, storing and transmitting FTI. For the annual assessment immediately prior to implementation of the IVR

system and each annual risk assessment (or update to an existing risk assessment) thereafter, the agency must include the IVR.

These requirements are explained in detail in the sections below.

#1 IVR System Architecture

The IVR system must be placed on a LAN segment that is firewalled to prevent direct access from the Internet. Because this LAN segment has no direct connection to the Internet, the risk of unauthorized access to the IVR system from external sources is minimized to an acceptable level.

The IVR application and related software must be hosted on a physically separate system from the database where FTI resides. The physical separation of systems into a two-tiered architecture can increase security of the environment because additional layers will have to be traversed to gain access to FTI. In a situation where the IVR software and database are located on the same host but logically separated, if that host is compromised, both tiers are vulnerable.

The **first tier (Application Tier)** is where the IVR system software and the processing of data and customer requests occur on an application server. This tier provides a layer of protection between the customers on the telephone and the FTI stored in the agency's database.

The **second tier (Database Tier)** is where the database server is contained that stores the FTI. The IVR application and related software must be hosted on a physically separate system from the database where FTI resides.

FTI must not be resident on the IVR application server after the data is passed through the system to the customer. The application must immediately delete any FTI that is stored on the server as part of a transaction.

The connection from the backend database to the IVR system must be encrypted as the FTI is transmitted between the two systems.

Access to the database from the application must be restricted to specific database tables, rows and columns that contain FTI and that access must be read only. There should be no ability to overwrite data in the database from the application.

#2 System Hardening

Each system within the architecture that processes, stores, or transmits FTI to an external customer through the IVR system is hardened in accordance with IRS Publication 1075 policy. The Publication 1075 policy can be met by utilizing the Safeguards Computer Security Evaluation Matrix (SCSEM) to configure the security settings for the applicable operating system and software that runs the IVR system. These SCSEMs are available for download from the IRS Safeguards web site

The IVR system must also provide role-based authorization capabilities for controlling access to its menu-driven administration utilities to authorized agency system administrators only.

#3 Risk Assessment and Vulnerability Scanning

Agencies are required to conduct a risk assessment (or update an existing risk assessment, if one exists) to assess the external and internal risk to FTI present in the system. Subsequently, the risk assessment must be reviewed annually to account for changes to the environment. The implementation and an evaluation of the associated risks should be part of the risk assessment.

Additionally, when FTI is provided to customers through an IVR, the required frequency with which agencies conduct vulnerability scanning of the IVR system architecture is increased to monthly to allow for more proactive vulnerability management of systems that provide FTI to the public via the IVR system.

#4 Customer Authentication

Callers to the agency’s IVR telephone lines to access FTI must have to pass a strong authentication mechanism. The authentication must use at least two pieces of information to verify the identity, one of which must be a shared secret only known to the parties involved, and issued by the agency directly to the customer. Examples of shared secrets include: a unique username, PIN number, password or passphrase issued by the agency to the customer through a secure mechanism. Case number does not meet the standard as a shared secret because that case number is likely on all case documents the customer receives and does not provide assurance that it’s only known to the parties involved in the communication.

For example, tax payers who call the IRS toll-free telephone lines are required to answer at least five but as many as seven questions before the assistor can discuss account information.

Resources

Additional information can be found in the following documents:

- IRS Publication 1075
- Additional Requirements for Publication 1075
- Recommended Security Controls for Federal Information Systems and Organizations, Revision 3" title="NIST SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations,* Revision 3">NIST SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations,* Revision 3
- Guide to General Server Security" title="NIST SP 800-123, *Guide to General Server Security*" NIST SP 800-123, *Guide to General Server Security*

References/Related Topics

- Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies and Entities
- Safeguards Program
- Additional Requirements for Publication 1075