Customer support and front-line call center staff have become the target for initial attacks or breach attempts at an increasing rate over the last few years. There has recently been a shift by malicious actors back to phishing, both through phone and email, to gain access to sensitive data. Several of the largest breaches in the last two years have been the result of malicious actors taking advantage of human nature, the desire to help.

This has caused many companies to reevaluate their security control posture and their risk. For quite some time, customer service teams were deemed to be lower risk than leadership or engineering teams, due to the thought that they do not have much access to vulnerable information. This is simply not true anymore. Many customer support teams have access to sensitive data, ability to reset users, and even internal support capabilities that allows for broad access. In fact, in several instances, the customer support team was called and convinced to install remote desktop tools that allowed the malicious actors to control their desktop and take over accounts.

With the focus from malicious actors shifting to call centers and customer support, what can an organization do? Below are the top five tips from a CISO on how to increase the security posture of your call centers.

# Email Security

Generic inboxes that send messages to tools like Salesforce or other CRM tools are a weak point for many organizations. Once the email is sent from your exchange server to that CRM tool, it is now outside of the control of your built-in phishing, malware, and spam tools. Due to this, it is important to focus on training your teams to understand that emails coming into the CRM tool or the customer queue are not always sanitized or safe. General best practices for email security still need to be followed. Further, an out of band process or procedure may need to be setup to account for triaging and remediating these emails in your CRM tool. It is recommended to look for a partner that can provide additional layers of security for your email system to help be more proactive in detecting and removing those malicious emails.

# VLAN Isolation

Having your call center operate on an isolated VLAN with limited access to systems and assets is another great approach. This serves as a two-fold benefit for your organization. First, it limits the access that a malicious actor could have if they were successful in phishing or social engineering. Second, if brand label credit cards are taken, it limits the scope for your PCI audit to that VLAN. In fact, it is recommended that if you are going to allow customer support to take brand label to limit it to a smaller set of people and have them on a smaller VLAN to further shrink scope and cost of your PCI DSS audit.

# SSO Integration

Much like VLAN isolation, this serves two purposes for your organization. First, this will enhance and improve the workflow for the call center. Having a single set of credentials that can access multiple systems provides for fewer password changes, password entries, and password reuse. In fact, many SSO capable solutions may limit the total number of requests for a user, because they are able to manage multiple authentications through session management. The second reason for this is that it will provide your security team a single point to review activity for users, to detect anomalous activity, and to quickly remove access. The more systems utilizing the same identity management system, the more efficient logging and behavior analysis is. Further, when a user leaves the organization, it streamlines account disablement to a single source rather than to disparate systems.

# Remove Local Admin

How often do your call center employees really need to install software? How critical is it to providing quality support to your customers? Odds are this will not be a big impact for your organization. To lower the impact of not having the ability to install or make system configurations, your organization can implement a curated list of approved software that can be installed (via a tool or self-service portal) for the end users. Odds are that your call center teams only need a few applications installed on the end point. The largest benefit to removing local admin is that is a common exploitation path in the attack chain. Many malicious actors and malware are looking to utilize the local admin rights to further their access and create a foothold on your network. Without entry, it helps to eliminate many attacks.

# Automated Payment Card System

The final recommendation is to utilize a self-service web or phone-based payment system. This not only limits scope for PCI DSS, but it also eliminates the risk of having helpful call center employees taking cards over the phone. The chances that numbers will be written down or added to notepad on the desktop are eliminated. These systems are extremely common these days, and most customers will have no issues with making payments in this manner.

With increasing attacks on call centers and customer support, it is important to not lose sight of the risk that can be introduced to the organization through your customer facing teams. While this article says top 5 tips, I cannot help but add one final item to never overlook. Quality security awareness training and phishing training is critical for your call centers. Ensure that everyone understands their role and the importance of operating a security program across the enterprise. As you look at your security program, continue to evaluate and assess the current threats that exist for your organization to properly implement security controls. There are many other tips that can be provided; these are just the top 5 from a CISO toolbox. They are meant to help limit scope in audits, reduce risk, and eliminate impact of breaches or incidents by shrinking the attack surface of your organization.