miratech

Call Center Cybersecurity Whitepaper

Call Centers: The Forgotten Target in Cybersecurity

Organizations today exist in an omnichannel world.

Unfortunately many of them have focused on protecting their online channels at the expense of their call centers.

Miratech has developed extensive expertise in the strategies, technologies, and solutions required to provide the highest level of call center security. Our global network has successfully secured many of the world's most hardened environments, among them the US Departments of Defense, Treasury, Homeland Security, and Transportation.

A timely response to a pressing need

113%
fraud rate increase

In recent years frequent targets of fraud like financial institutions, insurance companies, and others have concentrated their security efforts on their online channels. This has made online fraud significantly more difficult and risky for criminals to commit.

At the same time, however, fewer resources have been devoted to phone fraud. This, in turn, has made call centers significantly more vulnerable, a fact clearly not lost on those who would perpetrate it. In fact, from 2015 to 2016 call center fraud increased 113%. Everything from VoIP-, to SMS-, and to PRS-frauds contributed to the increase.

To cite some other disturbing numbers:

0.58$
lost per call

- In 2016, phone fraud cost companies 58 cents per call
- 41% of customers affected by call center attacks blame the brand
- Expired security certificates cost businesses $15 million per outage; 64% cannot recover in less than six hours

Basically, the increased investment in digital channel fraud prevention has driven more attacks to call centers. This is ironic, as cybersecurity assessments and training to secure call centers cost far less than paying agents and cybersecurity team to deal with cybersecurity issues after they occur.

41%
customers blame the brand

Among the problems, many legacy strategies have been easily evaded by social engineering, sophisticated spoofing, and SIM swap schemes. Most online fraud detection solutions still focus on point solutions for specific channels. And ever-faster automated attacks, which fraudsters modify as necessary to avoid detection, continue to put pressure on rule-based systems. The result is slower detection of new attacks and increased false positives.

Companies, of course, are not ignoring the threat. But frequently those tasked with call center cybersecurity are overworked, understaffed, and outmatched by the technical challenges of maintaining the highest level of cybersecurity.

Some of the challenges they face include:

15$ million
cost per outage

- Uncertainty their complex systems, including Genesys, are secure and an inability to monitor them properly
- The threat of data leakage and its potential impact on their business
- Finding ways to withstand Telephony Denial of Service (TDoS) attacks and what to do should they occur
- Absence of sufficient skills among their team to ensure their Genesys platform has been set up correctly and there are no cyber threats while it's operating

Here are some areas of concern:

Data Leakage

There are a variety of software solutions and technology platforms now available to gather, collect, and share customer information. While many of them have improved service efficiency and customer care, they have also opened up an increasingly large number of data exposure opportunities that can be exploited by criminals. This requires companies to deploy more effective security measures and data protection technologies.

Key to that is analyzing call center environments to determine factors such as the exact set of Genesys log files, configuration files, interaction recordings, and third-party integrations. Also critical is dealing with processing and storage of PII and other sensitive data, and conducting detailed assessments of vulnerabilities and threats.

In addition, increased outsourcing of call center operations has resulted in customer data being stored and managed all over the world. Attendant risks include call center agents being unaware of, or not trained to handle, potential customer data exposure. It can also result in service reps trying to take advantage of the accessibility of valuable customer information.

Just a few bad actors, in fact, can result in millions of dollars of both losses and fines. To combat this, agents and other call center employees should be required to be trained and pass certification tests on how to minimize the human factors that can contribute to data leakage and prevent human error.

There is also the problem of third parties tasked with developing IT systems or maintaining call centers not using the right security technologies. That can result in easy exploitation by hackers. Combating that requires thoroughly assessing third-party systems to see if they comply with security measures. If they don't, alternate technologies need to be identified on a case by case basis and then introduced into the call centers' operations.

Security Certificates

Call center security systems, particularly those based on Genesys security software, have to be continually updated. If a security certificate expires, it can take weeks of effort to get it back up, and result in downtime and millions of dollars lost to both fraud attacks and missed calls.

When some inexperienced or untrained managers find their certificates expired, they will sometimes do anything to get their systems back up and running, including deleting the expired certificates, and thus rendering the systems insecure. That is a breach of data protection regulations, which may result in significant fines.

Unfortunately, many managers responsible for call center security don't even know how extensive their Genesys systems are. For example, a typical Genesys client has roughly 100 security certificates, each with its own expiration date, and all of which have to be updated on a timely basis. That calls for both staying on top of certificate expiration dates and analyzing certificate storing procedures.

In addition to staying on top of expiration dates, it's essential to provide proper maintenance across the array of certificate types – from those that will not shut the system down to those that prevent any usage, identifying recurring certificate-related issues, and applying the right corrective solutions and maintenance procedures.

One way to do this is to develop specific guides for each team involved in certificate updates. Those teams can include Linux, Database, and Genesys engineers. Since each team has different understandings of certificate updating, they need a process that spells out precisely what each has to do in order to renew all certificates in a timely and efficient way. This can reduce the updating process from months to days.

User Access Control

Many companies often lose track of who has access to their data. Authorizations granted to an employee when he or she is hired frequently remain in force even when that person is no longer with the company. A white paper from Osterman Research revealed that 69 percent of organizations polled cited data loss when an employee leaves their organization.

Not staying up to date with who should, and shouldn't, have data access is essential to maintain call center security. This requires correctly applying all the user access management tools and policies like those available for the Genesys environment. Procedures need to be developed that can change user permissions without disabling service.

Such environments, when correctly deployed and maintained, identify potentially dangerous credentials, scripts, and configuration files and allow companies to take preventive steps before any serious damage occurs.

Telephony Denial of Service (TDoS)

Thanks to automation, Telephony Denial of Service, or TDoS, attacks are increasingly easy to mount and can create a degree of havoc well beyond the effort required on the attackers' part. If, for example, a flood of 20,000 unwanted, malicious inbound calls occurs instead of the anticipated 10,000 legitimate ones, it can swamp a call center's agents and hardware, ruining statistics and filling reports with wrong data.

TDoS attacks come in a variety of forms. Simple attacks come from a single point of origin, sometimes using spoofed phone numbers. The targets of this kind of attack are usually small organizations, since they rely on critical voice lines but likely have limited resources to respond quickly.

Complex attacks fly under the radar using spoofed numbers. They are hard to spot for both small and large companies.

Finally, distributed and complex attacks use highly sophisticated technology that makes calls appear to come from all over the country. Large companies with heavy call volumes that can't afford to lose legitimate callers are the most at risk. For them, early detection of TDoS attacks is critical. Doing so calls for a five-step process:

1. Verification of high availability configurations
2. Analysis of TDoS attack points of failure
3. Analysis of ability to determine attack parameters, such as TDoS target and source phone numbers
4. Analysis of current disaster recovery plan and scenarios, including component turn on/turn off sequence
5. Analysis of TDoS attack consequence management, such as WMF statistics

Misdialing

Another area that fraudsters have jumped on is misdialing on the part of consumers. In this attack, the criminals purchase phone numbers that are similar to those of a financial institution or other company.

When that number is dialed, a recording offers a call back. It also offers something to the customer, such as a free gift card, in exchange for information about their account such as their credit card number.

To guard against this, companies should investigate routing applications and log files to identify the root cause of misdialing. They must assess potential points of misdialing within their business processes, architecture, and routing strategies, and change their procedures as necessary. Developing specific procedures for both engineers and agents can also help avoid such issues in the future.

Best practice includes the audit of dialing all potential misdials and determining if any malicious activity is connected to potential numbers.

Missing Recordings

Call recordings are supposed to be for your protection. But often the recordings you need don't exist. Or the audio quality of the ones you have is too poor to be of use. Either way, you could not be able to properly serve a client, or even worse be liable for millions of dollars in regulatory penalties.

Whether you have the wrong backup mechanisms, poor storage management, or some other issue, a thorough assessment is needed to pinpoint the problem. That requires an analysis of solution architecture, component configurations, and third-party products integrations to determine the root causes of all reported cases, and determine recommendations to make sure the problem doesn't recur. More specifically, configuration verification of the recording solution in use, analysis of recordings search parameters, and analysis of problematic cases are necessary to develop corrective steps.

Taking these steps to identify specific cases of lost recordings can provide the insight needed to prevent them going forward.

Miratech CyberCX provides the highest level of call center cybersecurity, available anywhere.

Two thirds of all IT project fail, but 99% of Miratech's succeed, including Genesys cybersecurity projects.

Part of the reason is our extensive experience with Genesys beginning in 2000. Since then our more than 200 Genesys consultants have amassed over 3 million man-hours of Genesys expertise, supporting some of the largest companies in hospitality, banking and finance, telecommunications, energy, healthcare, insurance, and more.

To learn how we can bring the expertise that protects the most secure government and corporate environments in the world to your call center, please contact us:

+1 (202) 470 0845 info@miratechgroup.com www.genesys.miratechgroup.com