NORTH CAROLINA INFORMATION TECHNOLOGY SERVICES

SUPPLEMENTAL TELEPHONY SYSTEM GUIDE ON SECURITY

Securing Premise Equipment

State of NC
12/17/2013

Information related to reducing your risks and vulnerability to hackers seeking to steal long distance services by manipulating access to telecommunications equipment.

TELEPHONY SYSTEM GUIDE ON SECURITY

INTRODUCTION

Telecommunications access to telephony systems by unauthorized individuals has become an expensive activity. Unauthorized long distance calls often reaching to international locations have been thwarted in some cases but not detected in time in many instances. The first line of defense is a secure and correctly installed system that prevents scrupulous characters from pushing through the system using certain system features and gimmicks. Several hundred thousand dollars of illegitimate calls have been observed on a single system within just a few minutes by experienced and clever hackers.

A second line of defense exists with the AT&T contract that provides long distance service including international calls. AT&T monitors international calls to locations and numbers that have previously been found to enable fraud and illicit activity. However, they can't know new situations and patterns. Once improper calls are recognized, AT&T has been authorized to place a block on such activities until ITS resolves the issue. This "after-the-fact" blockage may still amount to significant costs and the customer is accountable for these costs.

SECURITY NEEDS

These security needs are not a new problem but appears to be on the rise. Often combinations of items that would allow security breaches are available to be discovered by the clever hackers. And just as often these "cracks in the wall" are not necessary for the proper operations of the customers/agency. It is just a matter of recognizing them and "plugging the holes". Here are a few popular methods. However, the equipment vendor will have the greatest expertise in securing the system and should be held responsible for making it happen.

1. System passwords for equipment as shipped from the factory will have well-known default passwords that should be changed to secure passwords upon installation. This applies to administrator passwords for Key System, PBX, VoiceMail, etc. Once logged in as the administrator, almost anything can be changed including how calls are routed when zero is pressed. It would be common for routing features to allow outside calls and enable long distance and international calls.

2. For hackers with certain knowledge, Auto-Attendants (AA's) have been known to allow access to outside lines. This can bridge the intruder out to make any type call.

3. Voice Mail systems may have the option to zero out to an operator. If no live operator is available, this may be directed to an Auto-Attendant (AA). As stated above, AA's often have the ability to transfer out to an outside line if you are familiar with the system as a hacker is likely to be.

4. Features assigned to station lines are often generously applied by default well beyond the needs of the users. One such feature is likely to allow the user to transfer the caller to an outside line. With a clever manipulation by the caller, the system switch may be able to transfer calls outside with "Trunk-to-Trunk Transfer". Once outside, the caller can access all long distance privileges.

5. Hackers can find ingenious ways to get passed the system and achieve their objective. Agencies are even more vulnerable when 1010xxx is used to dial around the picked carrier. When this happens, AT&T as our contracted service provider is not even aware of the activity and our contract arrangements with AT&T to monitor and block as necessary are not applicable. The agency is then left to the mercy of the carrier that received the dial around connection for such fraudulent calls. The agency is then liable for the costs. For this reason, all contracted providers for local service are instructed by contract to disallow and block attempts to use 1010xxx; and all ITS provisioned local lines are picked to AT&T Long Distance, the contracted provider.

KNOWN TROUBLE SPOTS

The following lists of area codes are known for their fraudulent activity. They can be reached from within the United States without dialing an international code. These codes carry a large amount of toll fraud and present a huge issue. They should be blocked on all systems and only allowed where a business case can be presented and secure procedures are in place. African and Asian nations (not listed) also experience significant toll fraud.

242 Bahamas
246 Barbados
264 Anguilla (split from 809)
268 Antigua and Barbuda
284 British Virgin Islands
340 US Virgin Islands: St Thomas, St John
345 Cayman Islands
441 Bermuda
473 Grenada
649 Turks and Caicos Islands
664 Montserrat

670 Northern Mariana Islands
671 Guam
758 St. Lucia
767 Dominica
784 St. Vincent and Grenada
787 Puerto Rico
809 Caribbean, Bermuda, Puerto Rico, Virgin Islands
868 Trinidad and Tobago
869 St. Kitts/Nevis
876 Jamaica
900 Pay-Per-Call Numbers
939 Puerto Rico
976 Pay-Per-Call Numbers

SECURITY DOCUMENTS

A recommended security check list is attached titled Voice Equipment Security Check List Aid for Initial Installation. The SCIO Statewide Information Security Manual document from which the check list below was derived can be accessed here: https://www.scio.nc.gov/library/pdf/Statewide_Information_Security_Manual_2013.pdf.

Also, a document from AT&T titled PBX (Private Branch Exchange) Security is attached.

PROACTIVE SECURITY CHECKS

In view of the increase in fraudulent attempts that have been observed, all agencies are encouraged to review their security preparedness and take steps to close any security holes. This may require the service of their equipment vendor.

Ignoring the security needs of their equipment may result in the agency being responsible for the high costs of fraudulent calling.

VOICE EQUIPMENT SECURITY CHECK LIST AID FOR INITIAL INSTALLATION

√	TDM Small System	Voice Mail Systems	TDM Large System	IP Telephony System	IP Based Adjunct Sys.		c=Customer v=Vendor	**REQUIREMENTS ABBREVIATED** **Note: Agency is responsible for full compliance with SCIO Security Standards via Agency Security Officer. Items listed are for Statewide Standards. Individuals are responsible for ensuring compliance to Agency Policies.**
	■	■	■	■	■	Operations	c	One or more responsible agency persons should be familiar with Security Manual with understanding sufficient for its application.
		■	■	■	■		c	Administrators will not extend network services without management approval.
		■	■	■	■		c	Administrators must obtain agency approval before using any security program or utility that will reveal State Network vulnerability.
	■	■	■	■	■		c	Only system administrators have access to operating system commands.
			■	■	■		c	Special administrative access is authorized by management with expiration date and removed when work is completed.
		■	■	■	■		c	Agency networks must be configured to safeguard the State's information systems using a layered Security approach.
	■	■	■	■	■		c	Agency must have trained administrators with documented and defined responsibilities for the system.
	■	■	■	■	■		c	System generated error logs must be regularly monitored and reviewed.
		■	■	■	■		c	Data storage must be protected and backed up to meet regulations including encryption.
		■	■	■	■		c	Agency policies/procedures must include State Network and data security vulnerability mitigation.
	■	■	■	■	■		cv	Security requirements shall be documented in an Under pending contract with service providers and monitored by the agency. Exceptions to security requirements shall be documented on the Security Form and then uploaded in the tool as processed.
		■	■	■	■		cv	System administrators ensure latest's security patches are applied and only essential application ports are opened in firewall.
	■	■	■	■	■		cv	System design information must be limited to persons for fulfilling operational duties.
		■	■	■	■		cv	System administrators must have management instructions, documentation and training.
		■	■	■	■		cv	External systems making connection must use agency approved antivirus and firewall protection.
	■	■	■	■	■		cv	With external system connections, internal administrative apparatus must timeout after 30 minutes or less with no activity.
		■	■	■	■		cv	Software upgrades must be pre-tested to ensure against security vulnerabilities and ensure operation as intended by design.
		■					cv	Auto attendant ports must be secured in the equipment to prevent hackers from placing fraudulent outgoing calls.
	■	■	■	■	■		cv	Passwords with 8 characters minimum and User IDs are required for System Administrators.
		■	■	■	■		cv	User ID and password is the minimum requirement for access to administrative management system.
	■	■	■	■	■		cv	Administrator passwords must be composed of random characters without spaces, must be entered manually and not displayed.
	■	■	■	■	■		cv	Administrator passwords must be changed at least every 60 days, and when compromised.
	■	■	■	■	■		cv	Any component taken out of service must have all data permanently removed by an approved wipe out utility.

		■	■	■	■	External Equipment	cv	State Network users with connections to external systems complies with State CIO's "Use of State Network and Internet Standard".
	■	■	■	■	■	Physical Access	c	Agency has written policies for physical access with safeguards in place that meet SCIO's Security Manual requirements
	■	■	■	■	■		c	Agency must safeguard sites, buildings and locations housing equipment.
	■	■	■	■	■		c	Equipment housing must ensure suitable environment and protect against conditions such as fire, floods, temperature extremes, dust, etc.
	■	■	■	■	■		c	Network and communications cabling must be secure and conduit protected.
	■	■	■	■	■		cv	Equipment has restricted physical access limited to required and authorized personnel
	■	■	■	■	■	Remote Access	cv	Remote access must be provided through approved modem pool or ISP via approved protocols.
	■	■	■	■	■		cv	Remote access must be through an agency managed secure tunnel that provides encryption and secure authentication.
	■	■	■	■	■		cv	Remote access to single equipment via Dial up is limited to agency employees and contractors (vendors).
	■	■	■	■	■		cv	Remote access to single equipment management consoles are approved by the agency security administrator.
	■	■	■	■	■		cv	Systems must log and maintain for 90 days remote user accesses with ID, date/time, and duration of connection.
		■		■	■	User Access	c	User with State Network access is controlled by User ID and Password that are unique to the individual.
	■	■	■	■	■		c	Agency has written policies for State Network user access.
	■	■	■	■	■		c	Agency has a backup system administrator for User ID and password management.
		■		■	■		c	Workstation screens must be protected with screen savers after 30 minutes of non-use and be password protected.
	■	■	■	■	■		c	Passwords with 6 characters minimum are required for users
	■	■	■	■	■		c	Inactive User IDs will be removed for all user interfaces.
	■	■	■	■	■		c	Password management must maintain secrecy.
	■	■	■	■	■		c	Malfunctioning systems must default to denial of user access privileges.
	■	■	■	■	■		cv	Passwords must expire and change regularly as defined by agency policy.
	■	■	■	■	■		cv	Unsuccessful log on attempts are limited to three when possible and such attempts are recorded.
	■	■	■	■	■		cv	Vendor-supplied default and/or blank passwords must be immediately reset as soon as equipment is installed.

PBX SECURITY: IT'S YOUR BUSINESS

PBX (Private Branch Exchange) Security

A PBX is a private switch that serves extensions in a business and provides access to the public switched network. If the PBX system is not maintained and secured, it can be an easy target for those with a mind to commit toll fraud.

PBX and Voice Mail Security Tips

❑ Run periodic security audits to check for loopholes in the PBX (have PBX vendor do this if possible)	❑ Restrict Toll Free dialing from areas where there is no business requirement.
❑ Disable DISA (*Direct Inward System Access*) if possible. If not possible, use maximum number of digits for DISA code.	❑ Frequently audit and change all active codes.
❑ Eliminate remote access to your PBX and disable access system	❑ Deactivate unassigned voice mailboxes and DISA codes.
❑ Do not allow unlimited attempts to enter system. Program PBX to terminate access after third invalid attempt.	❑ Do not allow phone lines to be "forwarded" to off-premises numbers.
❑ Shred directories or anything listing PBX access numbers.	❑ Make sure that system administration and maintenance port phone numbers are randomly selected, unlisted and that they deviate from normal sequence of other business numbers.
❑ Enable system lock-out feature on voicemail – this allows only X attempts at password before someone is locked out.	❑ Do not allow pass-through dialing
❑ Never divulge system information unless you know to whom you are giving it.	❑ Use random generation and maximum length for authorization codes.
❑ Secure remote maintenance port and use call back modem or alphanumeric passwords.	❑ Deactivate all unassigned authorization codes.
❑ Tailor access to the PBX to conform to business needs.	❑ Use multiple levels of security on maintenance ports (if available).
❑ Eliminate trunk to trunk transfer capability.	❑ Do not allow generic or group authorization codes.
❑ Restrict 0+, 0- and 10-1XXXX dialing out of PBX.	❑ Ensure that "Night Attendant" service does not default to dial tone when left unattended and change pass code on this line
❑ Restrict all calls to 900, 976, 950 and 411.	❑ Do not use "alpha" passwords that spell common words or names.
❑ Restrict 1+ dialing to extent possible.	❑ Immediately deactivate passwords and authorization codes to known terminated employees.
❑ Change passwords frequently.	❑ Consider implementing a *barrier code system*, i.e. an additional numeric password that adds a second level of security.
❑ Delete/change all default passwords.	❑ Restrict all possible means of out-dial (through-dial) capability in your voice mail system.
❑ Send e-mails out to all employees to change passwords on their voicemail (use longest passwords possible)	❑ Frequently change default codes/passwords on voice mailboxes.
❑ Restrict after-hours calling capability: DISA, International, Caribbean and Toll calls.	❑ Consider allowing only attendant-assisted international calling.
❑ Change passwords when there are personnel changes	❑ Delete all ex-employee voicemail boxes
❑ Analyze call detail activity daily (use SMDRs).	❑ Employ class-of-service screening to areas to which there is no business need to call.

IP PBX/Router Security Tips

❑	Contact your PABX vendor immediately to ensure all ports on the system are secure
❑	PABX – lock door; unplug when not in use; for remote access use VPN; keep log of authorized users
❑	VoIP – data network can be exposed to hackers, worms, viruses.
❑	Install Firewalls – hardware or software – inspects network traffic; denies/permits passage based on rules.
❑	Use Anti-virus programs
❑	Contact your PABX vendor immediately to ensure all ports on the system are secure

More voice mail security tips can be found here: ***http://www.fcc.gov/cgb/consumerfacts/voicemailfraud.html***. *More information about AT&T's NetPROTECT Family of Services may be found here:* ***http://www.att.com/business_billing/fd_fraud2.html***. *You may also contact your AT&T account representative or the AT&T* ***Service Establishment Group*** *at* ***1-800-NET-SAFE for more NetPROTECT info***.

AT&T Business Services – Global Fraud Management Organization (ABS-GFMO)
24X7 Fraud Operations Center: 800-821-8235

NOTE: *THE INFORMATION CONTAINED IN THIS DOCUMENT IS FOR AT&T BUSINESS CUSTOMERS AND IS FOR EDUCATIONAL PURPOSES ONLY. THERE ARE NO GUARANTEES MADE WITH RESPECT TO ITS ABILITY TO PREVENT PBX FRAUD OR ASSUME LIABILITY ON THE PART OF AT&T.*