Voice Mail Attacks Can Result in Costly Long Distance Charges and Toll Fraud

We have been receiving more and more reports concerning hackers accessing phone and voice mail systems and incurring expensive long distance charges. This is Toll Fraud - the theft of long-distance services by an unknown third party. It occurs when there is a security breach to your phone system or equipment, resulting in unauthorized long- distance calls which can result in severe charges on your account. It is a global, industry-wide issue with the potential to significantly impact your business – the most costly of which, is long distance charges.

Steps to Protect Your Business

Just as you would not leave the front door unlocked or the keys in your vehicle's ignition, your phone system must be appropriately secured. Below are protective measures you can take to reduce the risk of toll fraud.

Toll Restriction: International locations are a major destination for toll fraud calls.

- Recommended practice is to place a restriction on all international numbers and only enable those you need to call. Some systems allow for passwords to be required for long-distance calls.
- Work with your Telco provider to place restrictions on International Long Distance calls if your company does not regularly call International Long Distance.
- If possible, add Long Distance account codes to your phone system so that users/employees have to add a Long Distance code to access International phone numbers.

General Security: Develop Policies, maintain strong physical security, follow best practices for securing an IP-based service, monitor resources for new vulnerabilities, maintain patches and review logs. Consider utilizing standards-based security add-ons where possible.

- After Hours Calls: Restrict outbound calling after hours.
- Passwords: Immediately change the default passwords provided with your phone systems.
- Change user and administration passwords frequently. Change phone system passwords when key personnel leave your organization.
- Unused Mailboxes & Phones: When employees leave the company, remove their access from all phone systems immediately.
- External Transfer: Restrict call forwarding and call transfer features. Program your phone system so that extensions can forward only to known numbers and restrict all others. Never forward a caller to 901 or 90#.
- Software Patches: Make sure that your phone and voice mail systems are up to date and have all current patches installed.
- Monitoring: Monitor calling patterns and usage when using auditing features provided with your businesses phone system on a daily or weekly basis. Most toll fraud is generated in a short time – days to weeks and usually after hours when detection is least likely. Encourage employees to report strange languages on voice messages, especially those left after hours, or unusual and unexpected activity by the phone system (ie: all lines busy first thing in the morning).

- Social Engineering: Instruct employees to never give out technical information about your phone systems to unknown callers. Taking a moment to return a call can help to ensure you are speaking to the correct people.
- Formal Audit: Consider having an accredited, professional third party audit your phone systems to probe for any vulnerability that may have been overlooked or neglected.
- IP PBX phone systems: IP PBX's are susceptible to the same fraud issues as traditional phone systems. Additionally, they are also subject to security gaps in your data network. Control administrative access, user host-based intrusion prevention, and use network firewalls/intrusion prevention systems.

Voice Mail Best Practices

- When creating a new user, assign him a more complex initial PIN.
- Enable password aging.
- Educate your end users to change the default PIN to a more complex one (avoiding PIN with simple digit pattern such as 1111 or 4321 etc…).
- Check your CDRs (call detail records) regularly to detect any abnormal calling activities such as calls coming and going to a country you are not doing business with.
- If your business does not require international dialing, you can prevent international call back from voicemail by restricting the relevant user group to local and long distance calls only.
- Increase the voicemail PIN's length to at least 6 digits, system wide; Greater PIN length creates number combinations that make the attack more difficult.
- Enable email alerts for system event for repeated Voicemail login access failures.

ShoreTel Voice Mail PIN Codes Verification

ShoreTel users have a new application, named IDLint, available from Glenbriar Technologies or the ShoreTel support web site. The application will validate user PIN codes, identify users with weak PIN codes and incorporates options to improve PIN security of both voice mail passwords and conference host and participant codes.

Understanding Your Legal Responsibility

Securing your phone system is an imperative step in protecting your company from toll fraud. If a call has originated with or passed through your phone system or equipment, you are responsible for the charges associated with the call, whether the call is authorized or not. This means that if you are the victim of toll fraud, you are liable for the costs.

We highly recommend engaging the provider or maintainer of your phone system and equipment to learn how to prevent toll fraud. Ultimately it is your business' responsibility to ensure that your phone system and equipment are secure.

What to do if You Suspect Toll Fraud

1. Contact the provider/maintainer of your phone system immediately
2. Call your Telco provider or your long-distance provider immediately
3. Report the incident to your local police authority