InfoPlus
empowering
communications management

Customer Success Stories

Security Audit

Locking down your system

AVAYA Communication Manager

> *"Thank you so much for all you have done. The InfoPlus team got the audit taken care of amazingly quick. Once the audit was complete you went through and reviewed the information. You provided a summary of the best places to start our work, given the recent questionable call activity, and also provided a white paper on War Dialing. You even produced an updated copy of the audit after digging deeper on the "External References" section based on some questionable data that you noticed.*
>
> *I am very impressed with the speed and attention to detail that InfoPlus has shown. Your quality work is much appreciated. "*
>
> *Michael Bernardin*
> *Telecommunications Engineer*
> *Sheppard Mullin Richter & Hampton*

SheppardMullin

When communication system security is threatened, regain control with the InfoPlus Security Audit.

Sheppard Mullin, an international law firm with over 500 attorneys on staff, recently encountered a potential dialing hack on their Avaya Communications Manager. They quickly turned to their Avaya Business Partner, Windstream, to discuss potential options that would help them to analyze system programming and evaluate potential security risks. How could they quickly address this current threat to their communication system? How could they be proactive and prevent any future security problems?

Windstream knew that an InfoPlus Security Audit would satisfy their customer's needs. An all-inclusive InfoPlus Security Audit was run to identify potential security weaknesses in the system programming. This Audit provided Sheppard Mullins with the answers they needed to proactively address their current security issue as well as actions they could take to prevent future problems.

Challenge

It was clear that the Sheppard Mullin Avaya CM system was the target of a computer-generated dialing attack that started on a Saturday evening at 8:09 P.M. The following Monday morning, the intrusion was detected during a CDR review of the weekend activity. The records indicated that the main number was being dialed every minute with no caller ID information.

The system programming concerns were twofold: that this intrusion did not lead to toll fraud abuse, and more importantly, that there was no unauthorized access to the system that would in any way compromise business operations. Not knowing for sure the nature of this hack, they needed a way to analyze the system quickly to evaluate login credentials and all other associated programming that might be used to access external trunks.

Solution

After a brief conference call between InfoPlus and Mike Bernardin (Sheppard Mullin's Telecommunications Engineer), it was decided that in order to quickly evaluate the systems' security programming, an InfoPlus Security Audit would be run immediately.

That very night, InfoPlus polled the CM and obtained all the files necessary to produce a full-blown Security Audit, which was delivered the next day.

The InfoPlus Security Audit provided a thorough analysis of those critical features requiring evaluation - the potential sources for toll fraud abuse and login hacking.

This allowed Sheppard Mullin to quickly make necessary changes to their programming utilizing Avaya's Best Practice recommendations.

Results

- **Best Practice Lockdown.** Sheppard Mullin verified all relevant system programming, making changes where applicable, to ensure that the system was 'locked-down' and secure.

- **Timely.** In a matter of days, InfoPlus provided the customer with a thorough security analysis that allowed Sheppard Mullin to act quickly to minimize future risks.

- **Satisfied Customer.** Sheppard Mullin is confident that they have addressed all potential security risks in their system should another hack attempt be made to their system.

> *" One of the InfoPlus recommendations I immediately implemented was enabling the SVN (Security Violation Notification) feature. This whole experience not only forced me to analyze potential sources of toll abuse, but also made me think about the potential for future login hacking. With this feature now enabled, that threat can be managed more effectively."*
>
> *Michael Bernardin*
> *Telecommunications Engineer*
> *Sheppard Mullin Richter & Hampton*

InfoPlus
empowering
communications management

160 Summit Avenue Montvale, NJ 07645
(201) 746-7200

www.infoplusonline.com