The growing risk of a toll fraud attack is alarming with businesses facing bills which can run into thousands and even result in bankruptcy. It's a threat which most businesses don't truly understand or defend themselves against.

Defense against these attacks, however, can be resolved with a simple, low cost embedded solution - NEC's InGuard. This application is compatible with our SL2100 and UNIVERGE SV9100 communications platforms and provides a low maintenance, robust solution. And as one of NEC"s In-App solutions, it is embedded into your system, there's no extra cost and maintenance of a PC or server - unlike other solutions in the marketplace.

InGUARD SOLUTION

What Exactly is a Toll Fraud Attack?
This is a fraudulent attempt by a hacker to gain unlawful remote access to a phone system, usually via an open SIP port. Attacks are often highly organized from an automated server and once accessed, fraudulent calls are connected and over a period of time, can run up call charges of potentially thousands. Typically, these occur out of office hours and are usually discovered after the event, when it's too late and businesses are left to cover the costs.

How Does NEC's InGuard Defend Against these?
All call activity is monitored 24/7 and any suspicious call activity is detected instantly. This results is one of two automatic alerts: an 'alert only' email sent to designated recipients, or in more severe cases an 'alert and block' which prevents any further call activity instantly. The emails provide call information explaining why a call or calls were considered to be suspicious.

Once checked, if the call activity is legitimate the restriction can be removed simply by replying to the email and your business communications continue as normal.

InGUARD AT A GLANCE

> Monitoring of all call activity 24/7 offers instant detection of fraudulent activities
> Helps prevent toll fraud attacks which can easily cost thousands of dollars
> Provides two types of automatic alerts
> Complete call information is sent in the alert email explaining why a call or calls were considered fraudulent
> Embedded in and supported on NEC's SL2100 and UNIVERGE SV9100 communications platforms

www.nec-enterprise.com

How Does InGuard Work Specifically with Your Business?
The simple set-up of Toll Fraud is based around your business's specific call patterns, i.e. office hours, public holidays, length of a call, excessive calls rates, etc. From these parameters a set of rules are created - and if a rule is broken, an alert is sent. Not only does this detect a suspected toll fraud attack, it can also help prevent internal abuse of the phone system. You can make amends to your rule settings (e.g. changes in office hours) remotely via a browser for easy administration.

Does Your Business need InGuard Protection?
The vast majority of businesses are considered vulnerable to these attacks. Most networks and phone systems have only basic toll restriction features, and although no solution can provide 100% protection, the addition of a toll fraud application is strongly advised.

InGUARD
HEALTH CHECK FEATURE

During installation, this automated feature scans your overall system for any weaknesses with a 'traffic light' safety score. By identifying these security risks, the installation is then tailor-made for your specific system and network set up making it as effective as possible.

- Peace of mind with an effective toll fraud defense
- 'On duty' 24/7/365
- Helps prevent toll fraud attacks which can easily cost thousands
- Low cost on-board solution with no extra cost of PC server required (unlike other solutions in the marketplace)
- Tailored specifically to the needs of your business and call patterns
- Zero maintenance solution which 'sits in the background' – until any alerts are triggered
- Easy to use: alerts are easily switched off if telephone usage is legitimate
- Acts as a strong deterrent to internal telephone abuse
- Flexible solution with easy updates via online Application Manager
- Reacts instantly to a toll fraud attack

EMEA (Europe, Middle East, Africa)
NEC Enterprise Solutions
www.nec-enterprise.com

For further information please contact NEC EMEA or: