Background and description: Geo Risk Profiles

Webcall has several measures in place to prevent hacking and to reduce the impact of hacking on our clients. Geo Risk Profiling has also been added as an additional measure to limit the impact of possible hacking incidents.

General background on hacking:

How does hacking happen?

In most hacking incidents the hacker gains access to a device and then makes calls to very expensive destinations. The devices used may be telephones or PABXs. The expensive destinations are normally premium numbers in unregulated countries.

How to prevent hacking

Hacking is prevented in a number of ways, for example:

Restricting the access to devices:

- Restrict Internet access to devices by installing firewalls. This is complimented by the device's secure logon credentials.
- Separate the voice (telephones) and data (Internet) networks on client premises. Where the networks are shared a hacker might gain access to a phone via any of the on-site PCs.
- Webcall's core networks are protected by advanced firewalls.
- Foreign users are not allowed to register on Webcall's servers.

Even though vendors do their utmost to protect networks and clients from being hacked, the hackers constantly devise new and innovative methods to gain access. Vendors would then close the loophole; the hackers will try something new and the cat and mouse game will continue.

How to reduce the impact of a hacking incident

There is no 100% guarantee against hacking, even though all the possible preventative measures are in place. Vendors thus also need to limit the impact in the case of a hacking incident. Vendors are loath to share all their limiting measures in case the hackers devise new methods to circumvent a measure, but these are some of the well-known approaches:

- Blocking the numbers used by hackers prevent calls to these numbers. This is an ongoing process as new numbers are created all the time.
- Setting credit limits to limit a client's potential risk.
- Limiting calls to certain countries.
- Reporting suspicious traffic.

Geo Risk Profiles

Geo Risk Profiling is a tool that requires users to enter a 'one-time pin' on their phones when they make a call to one of the risky countries. Risky destination countries are those that have a very high ratio of hacking incidents.

The system, using IVR, will announce the reason for the interruption on the phone and request the user to enter a 3-digit PIN on, also on his phone (the system provides the PIN).

Note that destinations, by country, are divided into 3 risk levels, with actions as follows:

1. Countries with no restrictions: Calls are switched unrestricted.
2. Suspicious countries: The user will be requested to enter a PIN after the 3rd call to a suspicious country.
3. High risk countries: The user will be requested to enter a PIN before the 1st call to the country is switched.

The objective of this measure is to stop machines from making calls, assuming that the machine is not programmed to either understand or decipher the audio PIN request, while still allowing users to make legitimate calls to these countries.

Customising your Geo Risk Profile:

- Clients may request Webcall to customise their Geo Risk Profile if they have specific needs. Note that Geo Risk Profile is not call barring: With Geo Risk Profiling, calls may still be made to the listed countries, provided the PIN is entered when requested.
- Setting up and implementing a customised Geo Risk Profile will have a service fee of R768, excluding VAT. Once a customised Geo Risk Profile has been created and implemented, it may be updated for a fee of R280, excluding VAT.
- Please contact your relationship manager if you want to customise your Geo Risk Profile. You will need to provide the lists of countries that you want to categorise as suspicious and as high risk.

Please contact Webcall if you have any comments or queries regarding hacking or Geo Risk Profiles.