VTSL INSIGHTS

VTSL
Hosted Communications

SECURITY INFORMATION

A closer look at VTSL's security measures

VTSL goes above and beyond Ofsted's requirements to deliver robust security in all aspects of our service. We provide the security measures listed below for free to all customers, and review our security regularly to ensure best-practice.

ISO 27001

VTSL is currently undergoing ISO 27001 certification. ISO 27001 is one of the most respected information security standards in the world. It is recognised globally as a benchmark for good security practice and enables organisations to support compliance with a host of laws, including the EU GDPR (General Data Protection Regulation) and the NIS Regulations.

NETWORK SECURITY - FIREWALLS

The VTSL Ethernet router, which is provided for all Ethernet circuits, has a Linux firewall built-in. This firewall blocks all incoming traffic from the Internet to the LAN and allows all outgoing traffic from the LAN to the Internet in the default configuration. We can block incoming and outgoing traffic based on specific IP addresses, or range of IP addresses, depending on the requirements. VTSL's firewall is sufficient for majority of the use cases.

BARRING CALLS TO PREMIUM NUMBERS

VTSL is aware that many people do not log-in and out of their phones, and that in some instances it is simply not feasible. As such, as a default setting, we bar all calls to premium numbers. If a particular user needs to call a premium number, the customer's authorised administrator is the only person who can enable that by contacting our helpdesk. Once enabled, the ability to call premium numbers will be restricted to that user only. This policy can also be extended to bar calls to other numbers such as international numbers and mobiles.

NON-SECURE PINS

Many people tend to use PIN numbers that are easy to remember such as birthdays and other common patterns (i.e. 1234, 112233, 0101). VTSL has a security measure in place that prevents the system from accepting PIN numbers that fall into this category.

UNAUTHORISED USE OF PHYSICAL PHONES

Like voicemail, a minimum four digit PIN number is required for users to log in and out of their desk phones. PIN numbers protect against people who have authorised access to a building, but not the phones, from making outbound calls. (i.e. contract cleaners).

WEB PORTAL HACKING

At the web portal level the only way to hack in is through a brute force attack. To protect against this we have a three PIN lockout (PIN entered incorrectly three times) policy that will lock access to the portal completely. After this has happened the pin can only be reset by one of VTSL's support team. To unlock the portal, the customer's authorised administrator will need to contact VTSL's helpdesk. An email is then sent to the authorised administrator's email address with instructions for resetting the PIN.

NCC GROUP NETWORK TESTING

VTSL's network is externally tested for security threats by NCC Group. NCC Group is a global expert in cyber security and risk mitigation, working with businesses against the ever-evolving threat landscape. Should NCC Group see any weaknesses in VTSL's network, they are immediately highlighted so that VTSL can ameliorate them.

VOICEMAIL HACKING

A minimum four-digit PIN is a mandatory security policy implemented for all users that require access to the voicemail feature. Many phone systems have a feature called call back from voicemail and it is this particular feature that hackers utilise to make outbound calls to premium numbers. VTSL has always had this feature disabled on our network so all customers are protected against this threat.

ANTI-FRAUD DETECTION SOFTWARE

VTSL has anti-fraud detection software that alerts our support team against abnormal calling patterns. If we receive an alert, our helpdesk will immediately contact you to determine if this is a valid call. Additionally the software will alert our support team if a single call goes over a cost of £15. This value is configurable. Simply contact our helpdesk and we will make the change.