Case Study One – Client (Insurance Business)

Background

As the GM of one of the most dynamic insurance companies in the country with a passionate staff of 650 including industrial placement graduates Mr Dunstan has to be on top of his game. They had recently opened a new state-of-the-art ICT centre currently opened to staff and intend on giving public access for a fee in the near future.

Challenge

Mr Dunstan was initially alerted by a junior member of his management team about the amount of time some staff where spending in the ICT centre and there were other complaints that some staff where getting access to non-work related contents during working hours. Upon further investigation he found out that his IT manager could not identify the particular staff who had gained access non-work related content though the machine used was identified.

A senior manager who had supported the commissioning of the state-of-the-art ICT was concerned that some of the workstations were particularly slow and this was within a few days of the opening of the centre. Though they had AV installed on the workstations it took them two-weeks to realise that they had being infected with a malware which resulted in some workstations running slow.

Mr Dunstan, needed to address the issue urgently before the opening to the general public. He needed to be sure that he could rely on his IT department. He needed a solution that would provide security for his staff and the general public. He also needed a solution that would give real-time and comprehensive reports. Mr Dunstan turned to AchRock Technologies Ltd for assistance.

Solution

AchRock consultants ran a security audit on the network and identified a number of vulnerabilities. A detailed technical report was given to the technical staff at the ICT enabling them to fix the vulnerabilities whilst the management staff where given a summary report.

Their existing gateway solution was replaced with a UTM solution giving different security zones to staff, graduates on industrial placements, auditors and guests. Quotas where giving to staff ensuring that non-work related content could not be accessed once the allocated quotas were exceeded. After reviewing the security policy, strict content filtering policies were enforced at the gateway preventing users from accessing illegal and bad content.

The existing antivirus applications deployed on the workstations were replaced with a total endpoint security solution that featured program and application control, anti-malware and AV, firewall, media control and full-disk encryption.

Results

Improved network efficiency
Reduced cost of ownership
Improved security
Reduced risk
Increased user productivity
Reduced IT management time
Compliance
Real-time reports