



Secure Wireless Management

CASE STUDY

Code Red Systems Ltd.
21 HaVaad HaLeumi
POB 16120, Jerusalem, Israel
T +972-2-642-3401, F +972-2-678-3403
Email: info@code-red.biz
Web: <http://www.code-red.biz>

Philips Selects AirStop® Software to Prevent Wireless Bridging Attacks

Royal Philips Electronics is a global leader in lighting, medical devices, and consumer electronics. Headquartered in the Netherlands, Philips employs approximately 125,500 employees in more than 60 countries. The office in Yakum, Israel is responsible for the multinational's commercial activities in the Israeli market.

Overview

As in many high tech areas, system administrator Alex Zeifman, noticed that neighboring companies in the EuroPark high tech office complex had implemented wireless networks and even the coffee shop had a WiFi Hot Spot.

The Problem

Since all the company laptops had an enabled wireless connection, Zeifman became concerned about potential security threats. He then observed that users logged-in to the wired corporate network were simultaneously connected to neighboring wireless networks. It seems that the user-friendliness of Microsoft Windows' Wireless Zero Configuration coupled with the intelligence of Intel's Centrino chipset resulted in automatic connection to any wireless connection in range – without asking consent from, or notifying the user that a wireless connection was being made.

While authorized users innocently connected to the wired network using a standard Ethernet port, they were not even aware that their internal wireless card was connected to an external wireless network. From a data security perspective, simultaneous connection to two networks is a serious breach better known as "wireless bridging attack".

System administrator Zeifman immediately recognized the problem and set out looking for a solution.

"We looked at all types of profiling solutions," said Zeifman, "but realized that these could easily be circumvented accidentally or intentionally by our users which is not consistent with the strict enforcement of our data security policy."



Secure Wireless Management

The Solution

Recalling an earlier meeting with Code Red Systems at a wireless conference earlier in the year, Zeifman requested an evaluation copy of the company's AirStop Endpoint Security Software to see if it measured up to Philip's strict requirements.

The AirStop solution is designed to control the communications adapters and storage devices on a laptop or desktop computer. The software automatically detects all devices which are currently in use or have been used in the past. Using a password protected console, administrators are able to prioritize the various adapters and enforce security policy by enabling, disabling or "AirStopping" the various devices.

AirStop enforces security policy by preventing simultaneous connection to more than one network. If, for example, a machine is connected using a wired Ethernet connection, then AirStop automatically disables all other network connections including WiFi, 3G/Cellular, Fax/Modem and Bluetooth. There is nothing the user can do to enable these communications adapters once they have been disabled by AirStop.

If a user would like to switch from a wired connection to a wireless connection, then they must unplug the machine from the Ethernet and AirStop automatically re-enables the wireless connections. Once the user chooses a wireless connection, then all other adapters are disabled by the software.

In terms of storage devices, it is possible to disable them when connected to the network or define specific embedded codes which must be present on the device before it can be accessed by the user.

"AirStop is exactly what we were looking for.", said Zeifman, " It is simple to implement and can be distributed across the enterprise using a log-in mechanism or standard distribution platform such as Microsoft SMS. "

AirStop was successfully implemented at Philips and even helped cut down tech support by eliminating conflicts in the routing table between the various adapters.

Conclusion

As wireless networks become more popular, customers are looking for solutions which are manageable, secure and cost effective. While wireless communications increase mobility, they also provide new ways for intruders to gain access to sensitive information.

Profiling solutions may assist users in configuring their communications adapters, but when it comes to security, endpoint security software must be implemented in order to enforce corporate security policy.

About Code Red Systems:

Code Red is a software developer specializing in secure management solutions for 802.11 and 802.16 wireless networks. Headquartered in Jerusalem, Israel, the company has developed technologies which are used in field-tested solutions for solving the most pressing problems confronting wireless networking and security professionals today. For more information visit our web site at: <http://www.code-red.biz>