News

Tackling the Challenge of the Growing Cybersecurity Gap

The SolarWinds cyberattack of 2020 was cited by security experts as "one of the potentially largest penetrations of Western governments" since the Cold War. This attack put cybersecurity front and center on people's minds again.

The attack targeted the US government and reportedly compromised the treasury and commerce departments and Homeland Security. What's interesting about the SolarWinds attack is that it was caused by the exploitation of a hacker injected backdoor communications protocol.

This means that months ahead of the attack, hackers broke into SolarWinds systems and added malicious code into the company's software development system. Later on, updates being pushed out included the malicious code,creating a backdoor communication for the hackers to use. Once you hack one body, you can then gain access to many.

What has made the threat of cyberattacks much more prominent has been IT's growth in the last 20 years, notably cheaper and cheaper IoT devices. This has led to an explosion of network connected equipment. Compounding this issue is that IT spending has never really matched the pace of hardware and software growth. Inevitably, leading to vulnerabilities, limited IT resource and increase in IoT devices that now get more attention from would-be hackers.

In our view, this is the main reason why the **cybersecurity gap** is growing. As it inevitably boils down to counter-strike versus counter-strike. IT teams plug holes, and hackers find new ones, that is never going to stop. We must continue fighting cyber threats by developing new ways of protecting through in-house testing, security best practice sources, and both market and customer leads.

One of the key battlegrounds here is the education of end-users. This is an area where we see the battle being won at present. End-users' awareness of cybersecurity is increasing. It is crucial to educate end-users on what IoT devices are available, how they are configured, how to enable it effectively, and critically, how to use it correctly and safely.

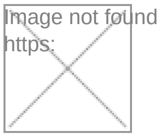
A valuable product that tackles cybersecurity, is **Razberi Monitor™**, which is new to **ComNet's portfolio**. Monitor™ is a software platform that provides a top-down view of the physical security network and ecosystem. It monitors and manages all the system components for cybersecurity and system health, providing secure visibility into the availability, performance, and cyber posture of servers, storage, cameras, and networked security devices.

comnet
Server Health
75%
IoT Health
81%
Cybersecurity Posture
67%
Offline Devices
Razberi Monitor™ Software
• Uptime Assurance • Cyberthreat Protection • Problem Resolution

By intelligently utilizing system properties and sensor data, **Razberi's award-winning cybersecurity software** prevents problems while providing a centralized location for asset and alert management. Monitor™ enables proactive maintenance by offering problem resolutions before they become more significant problems. Identifying issues before they fail and become an outage is key to system availability and, moreover, is a considerable OPEX cost saving.

Razberi Monitor is also full of features fully integrating with Razberi's hardware and custom cyber security offerings. Events such as; Brute-Force Attack, Denial of Service Attack, MAC Spoofing, Unauthorized device, whitelist and internet protection violations, Camera video and audio loss, IoT device excessive reconnects and switch statuses, as well as devices connecting to the network with common and default password are all detected. These cyber threat conditions are loaded and alerted live through the Razberi Monitor platform. Additionally, with Razberi Appliance defense we fully integrate the Cylance Protect AI Antivirus and Antimalware protection, meaning any software viral attacks are also alerted.

With Video Management platforms, **Razberi** has integrated the Milestone XProtect event platform into Monitor, meaning all above cyber threat conditions can be passed into the XProtect platform. In addition, all the XProtect alert events withing Milestone software can be passed out to the Razberi Monitor platform, making Razberi Monitor Cloud a one stop Cyber, Video health and systems health monitoring suite.



By Iain Deuchars

Iain Deuchars is the General Manager at ComNet International.