April 15, 2011

To: Check Point Software Technologies, Ltd. Utility Customers

This letter is in response to requests to clarify certain security features in Check Point products regarding Malicious Software Prevention requirements.

The following statements apply to all Check Point security gateway products that utilize Check Point Operating Systems, IPSO and Secure Platform.

Check Point switching, routing, and security products use specialized purpose built operating systems. The implementation or integration of any third party anti-virus or anti-malware software is not feasible. However, due to the unique nature of these operating systems, and the absence of outward facing software application interfaces, there are no known hooks for viruses to use to invade the system.

Further adding to the security of the system:

1. Firewall stealth rules block connections to the device
2. Appliances run a hardened OS. No unnecessary ports are opened on the appliance.
3. All traffic through the device is statefully inspected and checked against the rulebase
4. Traffic initiated from the firewall goes through the rulebase
5. Use of IPS on the device will detect / block any traffic that matches a vulnerability in the database or is a protocol anomaly
6. Connection logging is reliable and encrypted when delivered to the management system. Use SmartEvent to correlate logs to detect attacks
7. Admin auditing in CPSHELL/CLISH sends all admin commands to a syslog server
8. SNMP monitoring can be used to trap on unusual events and perform trend analysis to identify anomalous behaviour, resource issues etc.
9. Policy is not defined locally, but on the management.
10. Two factor / centralized admin authentication
11. System configuration can be reviewed quarterly by Check Point Professional Services to ensure compliance with industry best practice, latest threats, corporate security policy

I believe that this should address concerns regarding compliance to the Malicious Software Prevention requirement, as we are confident that these products provide very safe and reliable solutions for NERC / CIP implementations.

Best Regards,

Stuart E. Goodnick
Head of Solution Center Americas

