



The Perils of Mobility

In June 2005, when a computer worm attacked mobile devices for the first time in history, the technology industry was caught completely off guard. The worm, dubbed Cabir, spread via Bluetooth and infected cellular phones and other devices running the Symbian operating system. Luckily, the worm was harmless and did not wreak any widespread infections. Still, Cabir served as a wake-up call to CIOs and IT managers alike—at a time when the security of corporate information is of utmost importance. It proved that not even mobile devices are immune to attack.

Since the advent of Cabir, a number of other worms and viruses have attacked smartphones and other handheld devices. Because many business professionals check email and surf the Web on their mobile devices, these threats have jeopardized corporate security. In contrast to standard cellular phones, which usually store little more than phone numbers and addresses, new mobile devices may host any type of file that can be stored on a PC hard disk drive. Programs that give access to password-protected online services such as instant messaging can also be used on smartphones, which places confidential data at even further risk.

Currently, there is no threat of a global epidemic caused by mobile worms or viruses. However, this situation undoubtedly will worsen as mobile devices are shifted to standard platforms and virus writers find new ways to create chaos for the corporate world. Security experts at Gartner, Yankee Group, and a variety of other research firms predict that 2006 will be the year of the mobile-device virus. Rather than react to an outbreak after it occurs, network administrators should proactively work to secure mobile devices against malicious code before the next big threat materializes.

Controlling control

It's no secret that security is a balance between risk and accessibility. When administrators make the network more secure, it is harder for users to gain access. When they improve access, security usually drops precipitously. With this in mind, companies that allow employees to access their networks through personal digital assistants (PDAs) and other handheld computers need to require mobile devices to connect through separate firewalls. Wherever these firewalls are placed—on the network perimeter or on the devices themselves—they ensure that traffic is secure when it hits the network core.

The burden to control access does not only fall on corporate users—cellular and wireless service providers have the power to provide security, as well. Few present-day regulations require these companies to include any security provisions whatsoever. Many of these companies offer security, but customers have to pay separately for it. As mobile device worms and viruses become more prevalent, security likely is to become a key differentiator in the mobile market. Another way network administrators can secure their networks is by insisting that antivirus protection be part of their standard Service Level Agreements.



All about policy

Common sense dictates that a homogeneous network is infinitely easier to control than a heterogeneous one. Forward-thinking network administrators understand this inherently and make sure that they outline acceptable mobile devices from the very beginning. This task is harder than one might think, largely because many employees purchase their own mobile devices, so setting and enforcing mobile security policy can be next to impossible. Still, by establishing expectations early in the game, network administrators can eliminate this issue before it is even close to developing into a problem.

Once network administrators have set policy on acceptable mobile devices, they must communicate that policy effectively. For most IT organizations, communication consists of sending out a memo that users must read, sign, and return. In securing mobile devices, however, a more formalized education process is necessary to teach users why it is important to follow the rules. If one user fails to follow instructions, the entire network could be compromised. This makes it critically important that users understand which devices they can use when they interface remotely with critical company IT resources.

Be an architect

Finally, you cannot achieve unified security policy for mobile devices without designing a unified security architecture for your enterprise as a whole. In many cases, IT organizations have one group managing network security and another group managing mobile and telecommunications devices. This setup is a recipe for miscommunication and abject failure. The very best organizations have the same team of security professionals in charge of security for both the network and for mobile devices. In this way, companies can avoid having one security solution for mobile phones and another for everything else.

Architecting a strong behind-the-scenes defense is only part of the puzzle. For security measures to function most efficiently, companies also must deploy frontline defenses on mobile devices themselves. By supporting Pocket PC 2003 and 2003 Second Edition, VPN-1 SecureClient from Check Point Software Technologies enables PDAs and handheld computers to access resources protected by VPN-1 gateways. The solution maximizes endpoint security for mobile devices of every kind, making mobility a safer proposition for users and network administrators alike.

www.checkpoint.com/securitycafe

©2006 Check Point Software Technologies Ltd. All rights reserved. Check Point, Application Intelligence, Check Point Express, the Check Point logo, AlertAdvisor, ClusterXL, Cooperative Enforcement, ConnectControl, Connectra, CoSa, Cooperative Security Alliance, Eventia, Eventia Analyzer, Eventia Reporter, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Hacker ID, IMsecure, INSPECT, INSPECT XL, Integrity, InterSpect, IQ Engine, Open Security Extension, OPSEC, Policy Lifecycle Management, Provider-1, Safe@Home, Safe@Office, SecureClient, SecureKnowledge, SecurePlatform, SecuRemote, SecureXL Turbocard, SecureServer, SecureUpdate, SecureXL, SiteManager-1, SmartCenter, SmartCenter Pro, Smarter Security, SmartDashboard, SmartDefense, SmartLSM, SmartMap, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, SofaWare, SSL Network Extender, Stateful Clustering, TrueVector, Turbocard, UAM, User-to-Address Mapping, UserAuthority, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 VSX, VPN-1 XL, Web Intelligence, ZoneAlarm, ZoneAlarm Pro, Zone Labs, and the Zone Labs logo are trademarks or registered trademarks of Check Point Software Technologies Ltd. or its affiliates. All other product names mentioned herein are trademarks or registered trademarks of their respective owners. The products described in this document are protected by U.S. Patent No. 5,606,668, 5,835,726, 6,496,935, 6,873,988 and 6,850,943 and may be protected by other U.S. Patents, foreign patents, or pending applications.

Worldwide Headquarters
3A Jabotinsky Street, 24th Floor
Ramat Gan 52520, Israel
Tel: 972-3-753-4555
Fax: 972-3-575-9256
Email: info@checkpoint.com

U.S. Headquarters
800 Bridge Parkway
Redwood City, CA 94065
Tel: 800-429-4391; 650-628-2000
Fax: 650-654-4233
www.checkpoint.com

 **Check Point**
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.