



Check Point
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.



White Paper

A Getting Started Guide

What Every Business Needs To Know About Internet Security



Intelligent Security

Check Point protects every part of your network—perimeter, internal, Web—to keep your information resources safe, accessible, and easy to manage.

Contents

- 1 Overview: Internet Security In Small Businesses
- 2 Internet Access – New Business Opportunities
- 3 A Valuable Tool That Also Poses New Risks
- 4 Good Security Practices That Will Help Protect Your Network
- 5 Trusted Advisors
- 6 Summary

Overview: Internet Security In Small Businesses

Computer networks are powerful business tools, increasing worker productivity and enabling new ways for businesses like yours to get their products and services to market. But even a single computer connected to the Internet should have some form of security. So, the more your business relies on information and an Internet connection, the more important it is to put safeguards in place. What are those safeguards, and how can the average small business make sure it's properly protected? This brief Getting Started Guide from Check Point takes a look at what every small business needs to know about Internet security.

INTERNET ACCESS – NEW BUSINESS OPPORTUNITIES

Right now, with computer prices and Internet access fees more affordable than ever, the ability to connect to the Internet — or “get online”, is a very practical reality for small businesses everywhere. In fact, for many small businesses, connecting to the Internet is becoming a necessity — just like having a phone line, FAX machine and copier. Small businesses are using the Internet as a communications medium with business partners and customers, to increase awareness of their business and to shorten the sales cycle by providing information or even closing sales online.

A VALUABLE TOOL THAT ALSO POSES NEW RISKS

While the Internet is a powerful new business tool, it does pose some new risks for business. Some are merely annoyances, but others are potentially destructive and debilitating, and threaten the privacy and integrity of an organization's data and business.

Threats come from a number of sources including hackers, cyber terrorists and corporate spies, as well as disgruntled employees and under trained staff. While some of these groups may sound exotic and irrelevant to the average small business, the more malicious of the bunch are both clever and opportunistic, and are just as likely to target a small or large business as an individual. On top of that, inexperienced or poorly trained employees can contribute as much to risk as the other groups, simply because they don't know what the correct network security practices are, thereby creating openings for the others to exploit.

GOOD SECURITY PRACTICES THAT WILL HELP PROTECT YOUR NETWORK

Assess Risks

Any business connected to the Internet faces risks, which means every business using the Internet needs to understand the specific risks that are relevant to them so they can determine where to focus their security efforts. The process of answering the following questions will help businesses clarify the importance of their information resources and which of those need to be protected. Businesses should also consider contacting a trusted advisor (see section titled “Trusted Advisors”) for a complete and professional security assessment.

- What information resources need to be protected?
For example:
 - Do employee or patient records, bank account numbers, or plans and designs need to be protected?
 - Does your business need to comply with government or other regulatory requirements?

- What are those information resources worth?
- What threats do those resources face (e.g., damage, theft, tampering, etc.)?
- How likely are those threats?
- If those threats occur, what is the impact to the business (e.g., loss of future revenues)?

It's a good idea to specify in writing both your security goals or objectives and the plans to achieve them. This combination of information will form your company's security policy and should be communicated to all employees so they can understand the objectives, as well as how they can help reach them. The following sections discuss some of the procedures and tools businesses can put in place to reach their security objectives.

Precautionary Measures

Some of the basic steps a company can take to secure information include:

- **Back-up critical data**
Businesses should back-up their critical data regularly — weekly, daily or hourly if necessary, depending on how critical and dynamic the information is. The back-up process should be clearly documented and include the scheduled back-up times. It is also worthwhile to conduct tests, preferably at random times, to ensure the right data is being backed-up properly.
- **Regularly download and install security updates**
The most widely spread attacks, viruses, worms, etc., typically take advantage of well-known security holes in popular software programs. By simply downloading — and installing — security updates for your business software applications, you will be ahead of the game, and ahead of most of your competition. Of course, the same is true for every security product you use. Manufacturers continually update their security products, and keeping yours current is another simple way that you can stay ahead of increasingly sophisticated Internet-based threats. If there is one constant when it comes to information security, it is that security risks and threats are constantly emerging and changing.
- **Establish good password practices**
Because most hardware and software products come pre-configured with a simple and wellknown password, passwords should be changed from their default setting as soon as a product is installed. When selecting a new password, the choice should not be anything obvious, such as the person's name. Passwords should have a minimum length (typically 6 or more characters) and should contain numbers as well as letters. Once selected, passwords should be kept secret — and that includes not writing them on a scrap of paper attached to the computer monitor. Finally, passwords should be changed at regular intervals — once every few months is a good practice.

PROTECT YOUR INFORMATION

Firewalls

While most individuals are familiar with viruses and antivirus software, when it comes to protecting your business network, a firewall should be your first line of

defense. So, what is a firewall? Simply stated, a firewall is a security device that protects a computer network and resources on that network (PCs, servers, private data, etc.) by controlling access to the network.

More precisely, a firewall controls access by virtue of the fact that it is used as the gateway that connects two networks, usually the public Internet and a private business network. It examines all communications (e.g., email, web pages, file downloads, etc.) attempting to pass between those networks and, based on a security policy, decides whether to allow communications to pass or not. Your firewall's security policy should come directly from your business security policy — the plans your business puts in place to reach its security objectives.

TYPES OF FIREWALLS

Check Point introduced the first commercial, “shrink-wrapped” firewall over a decade ago. Today, there are numerous products on the market that offer businesses and individuals firewall protection. Still, the de-facto standard used by firewalls to enforce security policy is Stateful Inspection, which was invented and patented by Check Point Software Technologies Ltd. Stateful Inspection firewalls provide the highest levels of security for networks because they thoroughly examine each data packet and retain information about recent past communications. They use all of this information to decide if new communication attempts are legitimate.

Because firewalls are so important for proper business security, a number of ancillary products claim to offer “firewall features” as part of their capabilities. It's worthwhile understanding a little bit about these products to be clear about what they do.

One popular type of product on the market today is the PC firewall. These products are not true gateway firewalls in that they do not protect the whole network. Rather, they run on an individual computer and protect only that one computer. While useful for protecting a single computer, this particular type of firewall product becomes much less effective in a business environment with a network of computers. In these environments, having to install, configure and manage security software on multiple computers can become a huge administrative headache. If one person turns off or changes the security on their computer, overall network security can be compromised.

Another category of product, claiming “built-in security,” is the broadband networking device. These devices typically have a small subset of firewall features added on to their networking abilities. These devices do reside at the Internet gateway location, but they do not provide true Stateful Inspection-based firewall protection for your network. Most often, they simply employ a technology known as Network Address Translation or NAT. NAT helps hide the network addresses of your computers as they communicate on the Internet. By hiding the actual addresses of all your computers, NAT makes computers on your network harder for hackers to find, and thus more secure. NAT is an important security technology, but must be combined with Stateful Inspection and other capabilities for total firewall protection.

VIRTUAL PRIVATE NETWORKS (VPNS)

Firewalls protect business networks, but what protects business communications once they leave the confines of the internal business network and travel across the Internet — from business to employee or from business to business? This is a very important question for small businesses that have traveling workers, telecommuters, consultants or business partners that need to access the business network. The answer is “virtual private networks”, or VPNs. VPNs make your communications unreadable to others (i.e., “private”) as they flow across the Internet by encrypting information.

VPNs protect your business information when individuals such as remote and mobile workers need to access your business network, and when you need to connect your network to another network — such as branch offices or business partners — that needs to connect to your business network.

In addition to securing your business communications, VPNs can also dramatically cut your telecommunications costs. With VPNs, low-cost Internet access replaces dedicated dial-up phone line costs for connecting remote and mobile workers to the business network. And for connecting multiple business networks, point-to-point leased line connection fees are similarly replaced by low-cost, high-speed Internet access.

SECURE YOUR EMAIL

Email is the most common network-based application for most businesses. As a result, it is an often exploited conduit of security threats and nuisances. The most effective way to secure email is with antivirus security software. Antivirus manufacturers continuously track email-borne computer viruses and update their security products to neutralize virus threats before they infect your computers.

Antivirus software can be deployed to run on each individual computer with a corporation, and it can be deployed at a central location such as the Internet gateway. Check Point firewalls, for example, integrate with antivirus security software to block viruses at the Internet gateway, before they enter the network — simplifying administration and management.

Email that is virus-free can also compromise security. Mass distributed, unsolicited “junk” email, known as Spam, plagues nearly every email user. While Spam is typically used for advertising, if you respond to Spam in any way at all, you may be letting the senders know that they have reached a valid email address. That fact alone can be used not only to target you with more spam, but those with malicious intent could exploit it to launch additional attacks. So, it is generally a more secure practice to not open email — especially not email attachments — from strangers. As with viruses, anti-Spam products are available to manage Spam.

WIRELESS SECURITY

Wireless local area networks (WLANs) are increasingly popular among businesses of all sizes. They provide employees with a great deal of mobility and freedom at the business office, and consequently increased productivity. But wireless local area networks can represent a potential security risk as well. For example, people outside your business can try to connect their wireless devices to your network or monitor your WLAN traffic. So, it is important for businesses to secure their WLANs. An easy way to accomplish secure WLANs is to use a VPN in conjunction

with the WLANs. By using a VPN, communications on your WLAN will be encrypted.

EDUCATE YOUR EMPLOYEES ON SECURITY AND GOOD PRACTICES

Once you've spent the time to assess your security risks and devise your security policy, it is important to back your policy and plans up with good employee education. Every employee doesn't need to understand each security risk and how they are being protected, but it is important for employees to understand that they have an impact on network security, and how they can help. Whether it's proper password selection or good email habits, employees can make a significant difference in how secure yours/their business is.

TRUSTED ADVISORS

Understanding security risks and potential solutions can seem like a challenging undertaking. Fortunately, there are a number of businesses that specialize in consulting on security-related matters for small businesses. These organizations can help you perform risk assessments, craft security policies, select and install the right products and even help you manage your security policy. These businesses typically retain professionals that are certified security experts and can guide you through some or all of the areas outlined above. For a list of organizations that have partnered with Check Point to become security solution providers, consult the Check Point website at: www.checkpoint.com/sales, where you can find a local solution provider to help you.

Summary

With businesses relying more and more on their information assets and computer networks, network and Internet security becomes a necessity and not merely a "nice to have" item. From Internet attacks to email viruses, businesses need to understand both what to protect and how to protect it. And no business, no matter how small, should underestimate the need to assess their security needs, put proper security practices and procedures in place and educate their employees about network security.

About Check Point Software Technologies

Check Point Software Technologies Ltd. (www.checkpoint.com) is a leader in securing the Internet. It is a market leader in the worldwide enterprise firewall, personal firewall and VPN markets. Through its NGX platform, the company delivers a unified security architecture for a broad range of perimeter, internal, Web, and endpoint security solutions that protect business communications and resources for corporate networks and applications, remote employees, branch offices and partner extranets. The company's ZoneAlarm product line is the highest rated personal computer security suite, comprised of award-winning endpoint security solutions that protect millions of PCs from hackers, spyware and data theft. Extending the power of the Check Point solution is its Open Platform for Security (OPSEC), the industry's framework and alliance for integration and interoperability with "best-of-breed" solutions from over 350 leading companies. Check Point solutions are sold, integrated and serviced by a network of more than 2,200 Check Point partners in 88 countries and its customers include 100% of Fortune 100 companies and tens of thousands of businesses and organizations of all sizes.

CHECK POINT OFFICES:

Worldwide Headquarters:

3A Jabotinsky Street, 24th Floor

Ramat Gan 52520, Israel

Tel: 972-3-753 4555

Fax: 972-3-575 9256

e-mail: info@Checkpoint.com

U.S. Headquarters:

800 Bridge Parkway

Redwood City, CA 94065

Tel: 800-429-4391 ; 650-628-2000

Fax: 650-654-4233

URL: <http://www.checkpoint.com>

©2005 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, HackerID, 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, SmartL.SM, 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.

November, 2005 P/N 502040



Check Point
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.