Is your network an “opportunity” for a hacker?

Is Your Network An Opportunity For Hackers

Managed firewalls can protect your network

Managed firewalls are either software or hardware sourced (or a combination of both), specifically engineered to protect your network by preventing unauthorized access to it. Managed firewalls can prevent unauthorized access to your network

Essentially firewalls for networks and the Internet are much like firewalls in cars. They're designed to protect the people (or businesses) on one side from what disasters may occur on the other side.

Hackers are clearly honing their skills

Hackers are looking for opportunities across the breath of the Internet. If your network is vulnerable, trying to recover from an intrusion is a whole lot harder and more expensive than securely locking it down upfront.

Locking down your network can be a daunting task, and depending on an organization's expertise in Internet security, it's sometimes best left to professionals.

Could your business survive being hacked?

Obviously, if you're a major retailer pulling in millions in online revenues every quarter, your data is extremely important, but what if you're a small shop like a hair salon or a neighborhood hardware store? The question to ask would be, "If you lost your online business data or if it were somehow compromised, could your business survive?"

If you're not processing credit cards online and your website is simply informational, the protection offered by your hosting provider should suffice.

It's vitally important to protect your network

If your organization conducts business over the Internet, a managed firewall first and foremost protects your information and systems from compromise. It also ensures that any communication between you and your online customers is secure.

Set up protocols that limit access to all of your network devices including switches, firewalls, routers and intrusion detection sensors. Not all intrusions are malicious, but all of them compromise the security of your network's data.

ProlimeHost

Sales@ProlimeHost.com
+1 877-477-9454
www.ProlimeHost.com
Twitter: ProlimeHost

Managed firewalls can prevent unauthorized access to your network

Essentially firewalls for networks and the Internet are much like firewalls in cars. They're designed to protect the people (or businesses) on one side from what disasters may occur on the other side. Anyone who has read ancient history knows the dangers of a Trojan horse. Surprise! We're inside your network and we mean great harm. In Internet terms, a Trojan horse can wreak havoc on your network by injecting a type of malware that contains malicious executable code which all too often causes either theft of your data or harm to your system. As well, computer viruses and worms are responsible for billions of dollars in lost productivity every year.

Managed firewalls are either software or hardware sourced (or a combination of both), specifically engineered to protect your network by preventing unauthorized access to it.

Is your network an "opportunity" for a hacker?

Hackers are clearly honing their skills as we continue to see stolen credit card data from some major players, and we're talking now about intrusion attempts from all over the globe probing millions of networks for entry points. More often than not, it's not you they're targeting. They're looking for opportunities across the breath of the Internet. If your network is vulnerable, trying to recover from an intrusion is a whole lot harder and more expensive than securely locking it down upfront.

You know you need a firewall, but what's out there and how expensive are these protection solutions? I've sold firewall appliances for $5000 plus, but one size doesn't fit all. Should you incorporate packet filtering? Do you even know what that is? If a firewall keeps logs, could you or someone on your staff interpret that data? Locking down your network can be a daunting task, and depending on an organization's

expertise in Internet security, it’s sometimes best left to professionals.

First and foremost is the “worth’ of your business data

Obviously, if you’re a major retailer pulling in millions in online revenues every quarter, your data is extremely important, but what if you’re a small shop like a hair salon or a neighborhood hardware store? The question to ask would be, “If you lost your online business data or if it were somehow compromised, could your business survive?” If you’re not processing credit cards online and your website is simply informational, the protection offered by your hosting provider should suffice.

It’s shocking just how many WiFi networks are unsecured

Go into any industrial complex and I bet you’ll find more than one business with an unsecured WiFi network. I’ve personally seen as many as twelve unsecured networks in offices located in high rise complexes, for everything from doctor’s offices to law firms.

So many businesses purchase and install wireless routers, but never change the default password on that router, allowing intruders to re-route every outbound request from that network through servers in other countries.

It’s vitally important to protect your network

If your organization conducts business over the Internet, a managed firewall first and foremost protects your information

and systems from compromise. It also ensures that any communication between you and your online customers is secure. Obviously, it'll also significantly reduce the expense and disruption of your online operations caused by intrusion-sourced downtime.

If you've installed your own firewall

Rarely is it sufficient to simply install a firewall and walk away from it, expecting your network to be secure from then on out. Nearly every firewall logs all traffic that it blocks, and that traffic should be analyzed to determine if everything is functioning as it should be. Then, there's always the possibility that a defect in that firewall could result in its exploitation. More often than not, that occurs as a result of the firewall being misconfigured.

Our recommendation

Set up protocols that limit access to all of your network devices including switches, firewalls, routers and intrusion detection sensors. Not all intrusions are malicious, but all of them compromise the security of your network's data.

Brought to you by ProlimeHost

We've been in the web hosting industry for over a decade, helping hundreds of clients succeed in what they do best and that's running their business. We specialize in Virtual Private Servers (VPS) and dedicated servers, with data centers in Los Angeles, Denver & Singapore.

VPS Services: Lightning Fast SSD Virtual Servers

Our Virtual Private Servers all feature high performance Xeon processors and SSD storage in a RAID10 configuration to optimize your server's performance, which dramatically enhances visitor experiences on your site.

That speed is backed by unparalleled 24/7 support, featuring

both outstanding response AND resolution times to maximize your uptime.

Now is the time to join the ProlimeHost virtual private server revolution.

Dedicated Servers: Backed by a 99.9% SLA network uptime guarantee

We only use enterprise-class hardware in our dedicated servers and offer a four (4) hour hardware replacement. Throw in IPMI for remote management, support for public and private networks, free operating system (OS) re-installs, and SATA, SAS & SSD (including NVMe) storage. Call +1 877 477 9454 or email us at Sales@ProlimeHost.com. We’re here to help.