STRATiiS

Top 10 Ways Hackers Get Around Your Firewall

Provided by: STRATiiS Ltd
Author: Alun Borland

Cybercrime is at an all-time high, and hackers are setting their sights on small and medium businesses who are 'low hanging fruit'.

This report outlines the most common ways that hackers get in and details how to protect yourself and your business today.

Are You Protected?

The National Cyber Security Alliance reports that one in five small businesses have been victims of cybercrime in the last year – and that number is growing rapidly as more businesses utilise cloud computing, mobile devices and store more information online. You can't turn on the TV or read a newspaper without learning about the latest online data breach, and government fines and regulatory agencies are growing in number and severity.

I have outlined the top 10 ways that hackers can get in to your systems, with the goal of helping you to take the first steps in protecting your business.

10 Ways Hackers Get Into Your Systems

1. **They Take Advantage of Untrained Employees.** The #1 vulnerability for business networks are the employees using them. It's extremely common for an employee to infect an entire network by opening and clicking a phishing e-mail (that's an e-mail cleverly designed to look like a legitimate e-mail from a website or vendor you trust). If they don't know how to spot infected e-mails or online scams, they could compromise your entire network.

2. **They Exploit Device Usage Outside of Company Business** We advise that you maintain an 'Acceptable Use Policy' that outlines how employees are permitted to use company-owned PCs, devices, software, internet access and e-mail. We strongly recommend putting a policy in place that limits the websites employees can access with work devices and internet connectivity. It is important that you enforce your policy with content-filtering software and firewalls. We can easily set up permissions and rules that will regulate what websites your employees access and what they do online during company hours with company-owned devices, giving certain users more "freedom" than others.

3. **They Take Advantage of Weak Password Policies.** Passwords should be at least 8 characters and contain lowercase and uppercase letters, symbols and at least 1 number. Requiring a passcode to be entered on a mobile phone will go a long way toward preventing a stolen device from being compromised. Again, this can be enforced by your network administrator so employees don't choose easy-to-guess passwords, putting your organisation at risk.

4. **They Attack Networks That Are Not Properly Patched With The Latest Security Updates.** New vulnerabilities are frequently found in common software programs you are using, such as Microsoft Office; therefore it's critical you patch and update your systems frequently. If you're under a managed IT plan, this can all be automated for you so you don't have to worry about missing an important update.

5. **They Attack Networks With No Backups or Simple Single Location Backups.** Simply having a solid, reliable backup can foil some of the most aggressive ransomware attacks (this is where a hacker locks up your files and holds them ransom until you pay a fee). If your files are backed up, you don't have to pay to get them back. A good backup will also protect you against an employee accidentally deleting or overwriting files, natural disasters, fire, water damage, hardware failures and a host of other data-erasing disasters. Your backups should be automated and monitored; the worst time to test your backup is when you desperately need it to work!

6. **They Exploit Networks With Employee Installed Software.** One of the fastest ways cybercriminals access networks is by duping unsuspecting users to willfully download malicious software by embedding it within downloadable files, games or other "innocent"-looking apps. This can largely be prevented with a good firewall and employee training and monitoring.

7. **They Attack Inadequate Firewalls.** A firewall acts as the front-line defense against hackers; blocking everything you haven't specifically allowed to enter (or leave) your computer network. All firewalls need monitoring and maintenance, just like all devices on your network. This too should be done by your IT person or company as part of their regular, routine maintenance.

8. **They Attack Your Devices When You're Off The Office Network.** It's not uncommon for hackers to set up fake clones of public WiFi access points to try and get you to connect to their WiFi over the legitimate, safe public one being made available to you. Before connecting, check with an employee of the store or location to verify the name of the WiFi they are providing. Next, never access financial, medical or other sensitive data while on public WiFi. Don't shop online and enter your credit card information unless you're absolutely certain the connection point you're on is safe and secure.

9. **They Use Phishing E-mails To Fool You Into Thinking That You're Visiting A Legitimate Website.** A phishing e-mail is a bogus e-mail that is carefully designed to look like a legitimate request (or attached file) from a site you trust in an effort to get you to willingly give up your login information to a particular website or to click and download a virus. Often these e-mails look 100% legitimate and show up in the form of a PDF or FedEx tracking number, bank letter, Facebook alert, bank notification, etc. That's what makes these so dangerous – they look exactly like a legitimate e-mail.

10. **They Pretend To Be You.** Hackers pretend to be you to reset your passwords. In 2009, social engineers posed as Coca-Cola's CEO, persuading an exec to open an e-mail with software that infiltrated the network. In another scenario, hackers pretended to be a popular online blogger and got Apple to reset the author's iCloud password.

If you are concerned about employees and the dangers of cybercriminals gaining access to your network, then call us about how we can implement a managed security plan for your business.

Free IT Health Check

At **no cost or obligation** we will conduct a health assessment of your computer network and business technology. During this assessment we will analyse your network to identify vulnerabilities. Depending on what we uncover we will also make suggestions to prevent unauthorised access, augment security systems, better lock down sensitive data and overall, how to get more out of your existing technology infrastructure.

Our client risk report is included and provides an overview of the devices on the network along with a network Risk Score and analysis of each potential issue we uncover. We will review this document with you, discuss the findings and answer any questions you may have.

No-Obligation To Do or Buy Anything!

I also want to be very clear that there are no expectations on our part for you to do or buy anything when you take us up on our Free Health Check. Whether or not we're the right fit for you remains to be seen. If we are, we'll welcome the opportunity. But if not, we're still more than happy to offer this free service to you.

You've spent a lifetime working hard to get where you are. You earned every penny and every client. Why risk losing it all? Get the facts and be certain your business, your reputation and your data are protected.

Call us on 0141 348 7960 or you can e-mail me at aborland@stratiis.com

Alun Borland
Managing Director

Web: www.stratiis.com
Email: aborland@stratiis.com .