IT Defense: How to Protect All the Access Points

www.infinityinc.us

INFINITY

IT Defense: How to Protect All the Access Points

The Value of a Layered Approach

In the 1930s, France built a trench network called the Maginot Line to rebuff any invasion. The philosophy was simple: if you map out all the places an enemy can attack, and lay down a lot of men and fortifications at those places, you can rebuff any attack. Great theory. The problem is, you can't map every possible avenue for attack.

What does this have to do with IT security? Today, many business owners install an antivirus program as their Maginot Line and call it a day. However, there are many ways to get into a network that circumvent antivirus software.

Hackers are creating viruses faster than antivirus programs can recognize them (over 300,000 new virus types are released daily), and professional cybercriminals will often test their creations against all commercially available platforms before releasing them onto the Internet.

Even if you had a perfect antivirus program that could detect and stop every single threat, there are many attacks that circumvent antivirus programs entirely. For example, if a hacker can get an employee to click on a compromised email or website, or “brute force guess” a weak password, all the antivirus software in the world won’t help you.

There several vulnerabilities a hacker can target: the physical layer, the human layer, the network layer, and the mobile layer. You need a defense plan that will allow you to quickly notice and respond to breaches at each level.

95%

of security incidences involve human error

11.6 million

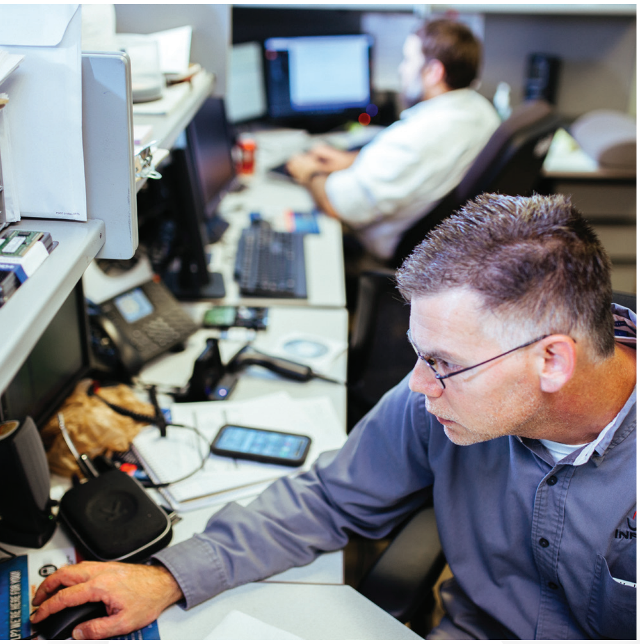
infected mobile devices at any given moment

The Physical Layer

The physical layer refers to the computers and devices that you have in your office. This is the easiest layer to defend, yet it is exploited surprisingly often.

Here are a few examples:

- The breaches perpetrated by Chelsea Manning and Edward Snowden occurred because they were able to access devices with sensitive information.
- Recently 60% of California businesses reported a stolen smartphone and 43% reported losing a tablet with sensitive information.
- Comptia left 200 USB devices in front of various public spaces across the country to see if people would pick a strange device and insert into their work or personal computers. 17% fell for it.



"Start by protecting your hardware and devices."

To protect the physical layer, you need to:

- Keep all computers and devices under the supervision of an employee or locked away at all times.
- Only let authorized employees use your devices.
- Do not plug in any unknown USB devices.
- Destroy obsolete hard drives before throwing them out.

The Human Layer

The human layer refers to the activities that your employees perform. 95% of security incidences involve human error. Ashley Schwartau of The Security Awareness Company says the two biggest mistakes a company can make are “assuming their employees know internal security policies and assuming their employees care enough to follow policy.”

34 out of 200
people picked up an unknown USB device and used it

Here are some ways hackers exploit human behavior:

- Guessing or brute-force solving passwords.
- Tricking employees to open compromised emails or visit compromised websites.
- Tricking employees to divulge sensitive information.

To protect the human layer, you need to:

- Enforce mandatory password changes every 30 to 60 days, or after you lose an employee.
- Train your employees on best practices every 6 months.
- Provide incentives for security conscious behavior.

- Distribute sensitive information on a need-to-know basis.
- Require two or more individuals to sign off on any transfers of funds.
- Watch for suspicious behavior.

"An effective defense requires an informed general who can direct resources where they are needed most."

The Network Layer

The network layer refers to software attacks delivered online. This is by far the most common vector for attacks, affecting 61% of businesses. There are many types of malware: some will spy on you, some will siphon off funds, some will lock away your files. However, they are all transmitted in the same way:

- Spam emails,
- "Drive by" downloads on compromised websites.

To protect against malware:

- Don't use business devices on an unsecured network.
- Don't allow foreign devices to access your wifi network.
- Use firewalls to protect your network.
- Make your sure your WiFi network is encrypted.

- Use antivirus software and keep it updated. Although it is not the be-all, end-all of security, it will protect you from the most common viruses and help you to notice irregularities.
- Use programs that detect suspicious software behavior.

The Mobile Layer

The mobile layer refers to the mobile devices used by you and your employees. Security consciousness for mobile devices often lags behind that on other platforms, which is why there 11.6 million infected devices at any given moment.

There are several common vectors for compromising mobile devices: traditional malware, malicious apps, and network threats.

To protect your mobile devices you can:

- Use secure passwords.
- Use encryption.
- Use reputable security apps.
- Enable remote wipe options.

Our Layered Approach

Business security and data protection cannot be accomplished with a simple padlock. The varying number and types of threats, combined with all the different ways that data can be accessed or exposed, requires a multifaceted approach. This is why we layer our security, providing level upon level of protection. If you're curious to see how our security can guard your critical data, give Infinity Inc. a call.

INFINITY

10 Chatham Center South Dr.
Suite 300
Savannah, GA 31405

912-629-2426
info@infinityinc.us