Background Security: Anti-Virus/Anti-Malware & Firewalls

Dray Agha / 04 May 2020

Anti-virus/anti-malware and **Firewalls** are security features that run in the background of our devices, and can sometimes stay in the background of our thoughts when we think about our cyber hygiene. There are a lot of myths and **rumours** associated with these protections, so let's examine how they work and the things they **can't** do.

Anti-Virus / Anti-Malware

Anti-virus (AV) and anti-malware (AM) protection are two distinct things.

- AV is mostly effective on the more 'classic' types of attacks, but **new attacks may not yet be on the AVs watchlist.**
- AM tends to be more clued up to **the latest attack trends**, but may not offer protection against classic, more mundane malware.

They both keep an eye out for the tactics, payloads (malicious code), and origins of attempts to infiltrate your computers. And then they thwart those attempts. They aren't perfect however, as hackers are always coming up with **new methods to bypass AV/AM protections.**

Running both AV and AM at the same time sounds like it should be a great idea, but it isn't! They would clash, cancel each other out in places, and make your computer slow. It's better to have a consistent AV running, and to **only run AM periodically** or when you think your computer is acting unusually.

It's hard to recommend any one company's services, as it really is specific to your business use. You will have to do some homework and find an AV and AM that are best suited for your case. There are some things to keep in mind when you're looking:

- There are providers who offer **both** AV and AM services.
- **Free** does not mean an AM or AV service will be bad.
- It's best to read the description of the protection product you'll be choosing, to make sure you're picking what works for you. Picking what's most expensive isn't always appropriate for your business if **it includes some features you won't need.**
- Some AVs have been accused of **cyber espionage**, on behalf of other nation-states.

There is a persistent rumour that 'Apple devices don't get viruses'. **This was *once* a half-truth**. In the past, Microsoft Windows was more common worldwide and it made sense for hackers to craft attacks for Windows specifically. Apple devices have a different underlying structure to Windows, and hacks for one can't just be used on the other.

> *"For the first time ever, Macs outpaced Windows PCs in a number of threats detected per endpoint" – Malwarebytes, 2020 State of Malware Report*

However, as Apple devices have become more popular, **hackers have paid more attention** to crafting attacks for MacOS. Apple do go to great lengths to have built-in security mechanisms, such as not letting unvetted software on the App Store. But **it's still advised to get anti-virus and AM for your Apple devices.**

Firewalls

The purpose of a firewall is to be the *wall* of protection that **separates** your computer and hackers who want to ruin your day. Firewalls **determine the origin of incoming** data and do their best to block dubious packets that want to get through the wall.

Clever attackers will try and disguise their dangerous malware to look like authentic data transfers from the web **–** the hacker may try and pretend their payload is a Microsoft Word update, for example. A firewall makes sure that your Microsoft Word update is exactly that, and blocks a hacker whose dangerous payload is masquerading as a Word update.

A firewall can stop your programmes from working sometimes. But some hassle to **make both firewall and program work is always preferable** to turning the firewall off to make the programme work. Firewalls are extremely necessary as hackers automate their attacks to scour the globe, looking for devices that are vulnerable. One such vulnerability they look for is if the firewall is turned off, or poorly configured.

Firewalls exist in your computer, and can exist in your Wi-Fi router. It's always a good idea to **check on the firewall configuration** in all devices you own. For personal computers, the average built in firewall should be just fine. However, for some business cases, you may want to explore third-party firewalls. Some companies offer AV, AM, and Firewalls all in one package, which may be an option for you.

One of the downsides of firewalls is that their interfaces are not that friendly. Whilst AV/AM looks easy to use and easy to use with a click here and there, **firewalls can become complicated quick,** with different rules for inbound and outbound connections. It's best to **confer with someone experienced** in firewall rules before you configure them yourself.

Security in the Background; The User up Front

Firewalls and AV/AM share in some of the things they 'can't do', which all revolve around how proactive you are about your cyber security.

- **Bad passwords:** poorly chosen passwords, or using default credentials that devices and services come with, gives an attacker an open door through your protections, as they have found 'legitimate' access and do not need to send an attack.
- **Social engineering:** these protections are of little help with email scams or telephone scams. Email-filters and training are your only protections here.
- **Poor security configurations:** protections can be undermined if you turn them off, or if you do not update them or other software on your device, as attackers can exploit these unpatched services.
- **Unverified software:** software that has been pirated or downloaded from unverified sources can be riddled with malware, and gives the hacker a method of attack that can bypass the protections.
- **Sophisticated attacks:** targeted attacks by sophisticated, well-funded hackers are very unlikely but still a possibility. These hacking groups are very capable of bypassing many protections.

Hackers prefer easy targets and will give up and move on if faced with obstacles. By ensuring that your background protections of AV/AM and firewalls are optimised for your business purposes, you are making the hackers job that bit harder.

Further guidance:

- https://www.ncsc.gov.uk/guidance/what-is-an-antivirus-product

Dray Agha is a PhD Researcher based in the Information Security Department at Royal Holloway University of London