"Follow The Data"

Get GDPR Penetration Testing
Working for You

Are you planning to perform Penetration Testing to meet GDPR?

Yes…

Here, we answer a few questions to help you get the best value for money.

First and obvious question. *Do I really need to test?*

Ask yourself if you have personal data being processed on any computer system. If you don't, the answer is no. However, most organisations will process some personal data and therefore must secure it.

If you have not already done so, understand what personal data you process. This should be one of the first GDPR tasks you complete. You must understand what is processed before you start to protect it.

Ok, so let's assume you do process personal data.

One of the main GDPR requirements is to keep personal data secure.
Existing security standards such as ISO 27001 and PCI DSS require that you perform penetration testing.

Testing should review the security of important networks and applications. It should be performed periodically or after a network is changed or upgraded.

As a rule of thumb test at least annually. Retain all evidence of testing and resulting improvements to show you are working to GDPR. This will be an important step in demonstrating your commitment to keeping personal data safe.

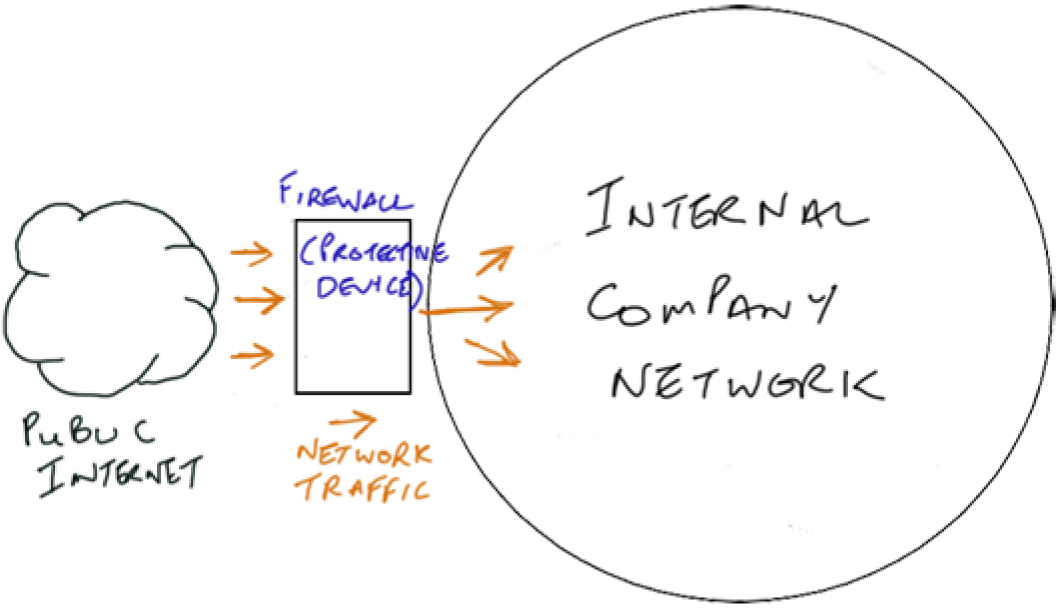
What should be tested?

This is the question we get asked the most.

There are security standards such as PCI DSS that have a clear requirement about what needs to be tested. For example, PCI DSS is designed to protect payment card data. It focuses on networks that store, process or transmit payment card data. This includes internal networks and areas that face the public Internet.

A similar model can also be applied to GDPR.

Where you process personal data forms the target for your GDPR penetration test. This includes both the internal network and any Internet facing routes into that network.



A practical way of looking at this is understanding how a data breach might occur. For example, personal data sits on your internal network. A hacker tries to access this data by working around your external facing network, then through your internal network.

Two stages. External followed by internal attack.

Use this same approach with developing your penetration test plan. As a result, testing becomes an extremely useful security tool rather than a ‘tick-box’ exercise.

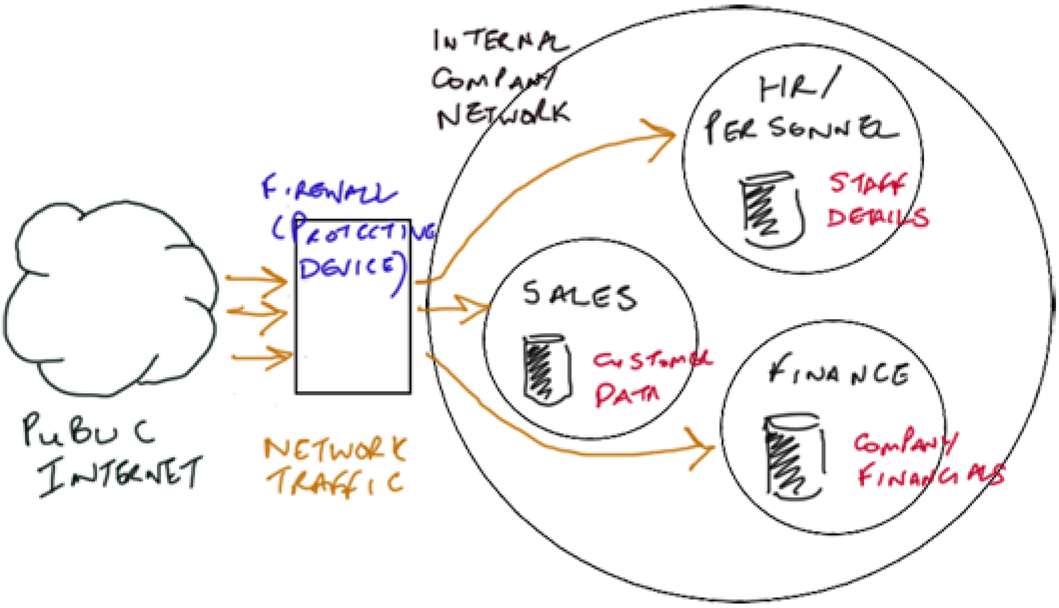
Where should I begin?

You will need to perform some initial leg work. Understand where all personal data is being processed. Start by finding out where it is stored.

As well as your internal systems, be sure to include cloud services like Google G-Suite, Office 365, Dropbox, Salesforce and so on.

It is widely accepted that a flat, wide open internal network is not a good idea. This provides staff with full access to all data and services.

Often organisations create sub-networks or other access policies that support specific business functions. For example, a Finance or HR network. This helps to restrict access to the right people.

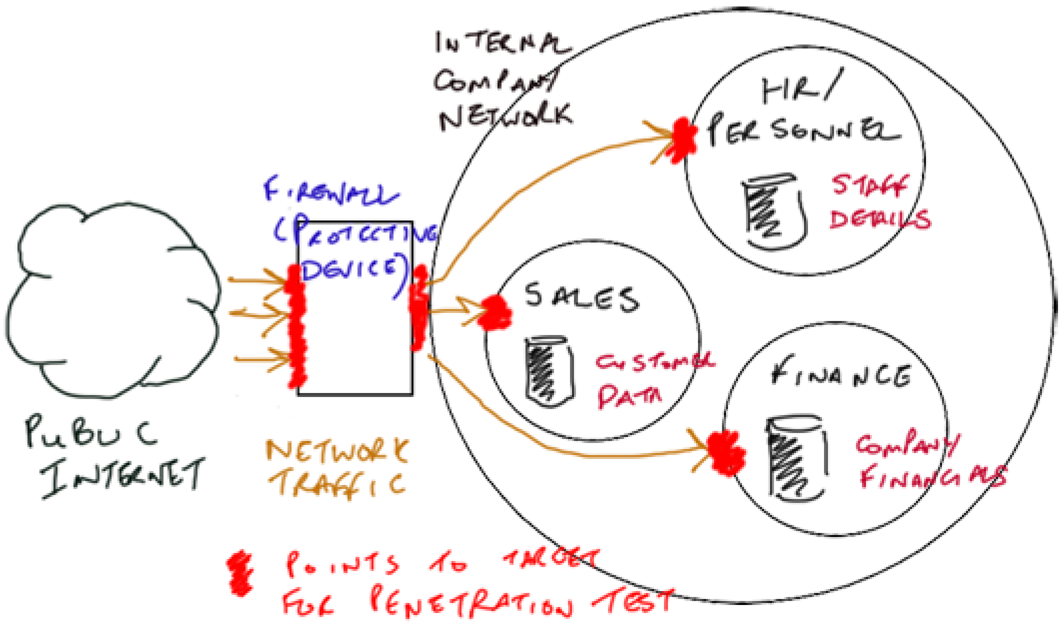


If your networks are segmented in this way, the perimeter of each one becomes the scope for the penetration test.

Testing can demonstrate how effective these control measures are at allowing only the right people in.

Next, understand where your network meets the public Internet. This could be through a firewall or a web application. These should be in scope for the penetration test.

By identifying a complete scope that includes both internal and external targets, you will more *accurately test how an attacker will try to access your personal data*.



Always bear this in mind when performing security reviews.

Yes, you should comply with legislation. However, always have a keen eye on how your network might be breached and data lost.