pentest
INFORMATION SECURITY ASSURANCE

Pentest_guide

protecting your
company's crown jewels

pentest
INFORMATION SECURITY ASSURANCE

don’t let hackers hit you in the crown jewels

The increase in GDPR fines has rightly brought the issue of information security to the top of many company’s agendas, with most taking the necessary steps to improve security around personal data.

GDPR fines are extremely serious and every business should be complying with their legal requirements, but for many companies GDPR fines may be the least of their worries when it comes to potential information loss.

What would happen if an attacker was able to gain access to a company’s crown jewels, the critical assets, data and sensitive information that a company relies on to operate?

The impact could go beyond monetary fines and, in the worst cases, may even threaten the future of the business.

So, how do you ensure your company’s crown jewels are protected from such threats?

0ur guide is here to help you.

pentest
INFORMATION SECURITY ASSURANCE

step 1: identify what’s important to you

Email is often seen as an important component in the day to day operation of a modern business. But what would happen if email servers went down? It would undoubtedly cause problems; however, you would hopefully have contingency plans in place to allow your business to continue operating whilst the problem was rectified.

A company’s crown jewels aren’t just important, they’re critical and if they were stolen or made unavailable, for even the shortest time, it could mean huge financial loss and potentially jeopardise the business itself.

But what are your crown jewels?

For many it’s intellectual property (IP), such as the design of a new product or your ‘secret recipe’, for others it could be financial data. Maybe it’s the source code you’re developing for a big client, it could be an algorithm you’ve developed, patient information, your production systems, the servers running internal operations, or it could be your transactional e-commerce website.

It can be a combination of things, but whatever it is, it needs protecting.

The key question you need to ask yourself is; what’s the thing/s I can’t afford to lose?

pentest
INFORMATION SECURITY ASSURANCE

when attackers strike IP gold - the Codan story

In 2011, Codan, an Australian metal detection and mining technology firm, realised it had a major problem. It had started to see an unusually high number of faulty metal detectors returning to its service centres, but the number of faulty products wasn't the issue.

When service staff looked inside, they found that the detectors weren't their products at all, they were counterfeit products that had been built using inferior parts.

It turns out that an employee's laptop had been compromised whilst connecting to an unsecure hotel wi-fi network during a business trip to China. With access to an account, attackers were able to access product blueprints during development and pass these on to Chinese manufacturers, who then flooded the market with the cheaper counterfeit products.

Codan had to act quickly, slashing their prices from $4,000-$5,000 to $2,500 in an effort to compete and the company spent a 'significant amount' of money establishing the identity of the perpetrators.

Jail terms were eventually handed out to those responsible, but the damage had been done.

-$35.8m

Codan's net profit fell from $45m in the previous year to $9.2m.

pentest
INFORMATION SECURITY ASSURANCE

step 2: build your defences

Now you've identified your critical assets and sensitive data, you need to start building up your defences around them. Whilst nothing is '100% unhackable', the more effective defensive measures you put in place, the more you deter would be attackers.

Time and budget constraints are always going to be a factor in your information security efforts and most companies will have limited resources with which to work with. When this is the case, your focus needs to turn to protecting your crown jewels.

But what defences should you be putting in place? We give you our information security best practices:

Segregate your networks and lock your crown jewels away

In the days before information technology, companies who wanted to keep their secrets protected often locked them away in a secure place, with only a few select people having access. For some companies that's still the case and it's said that KFC keep their secret recipe in a safe monitored by 24-hour surveillance and that Coca-Cola keep their recipe locked in a secure metal box, within a high-tech vault.

For most businesses, a physical safe just isn't feasible for their 'online' or technology based critical assets. But the principal remains the same; put your most important assets somewhere safe and restrict access to them.

But how do you do this?

Firstly, you will want to segregate your network and move your critical assets away from the rest of the day to day operations.

A flat network can be an attacker's dream and any beach could allow attackers easy access to sensitive data, without the need to jump between networks. By segregating your network, you make the job of the attacker more difficult and increase the chances of their activity being discovered.

Once your network is segregated, you'll then need to restrict access. There are several ways you can do this:

> Tighten user permissions/privilege levels

What information do your staff have access to? And do they really need it?

When it comes to sensitive information, access should only be granted to those that really need it. Does the marketing team really need access to finance's data? No. Does the reception team need access to IT's data? No.

Privilege levels can often go years without review, and it can mean that staff, especially those who have moved around within the company, have access to far more information than they should. This can be a dangerous situation and if a staff member's account was to be breached, it would give attackers free access to that information.

By keeping close control over permission levels, you restrict what a member of staff, and ultimately an attacker, can gain access to. Reducing the likelihood of sensitive information falling into the wrong hands.

> Utilise multi-factor authentication

Two factor authentication is starting to see widespread adoption and by requiring multiple authentication methods to access sensitive data you make life more difficult for a potential attacker.

Even if an attacker did manage to gain access to your internal infrastructure, multi-factor authentication would slow their efforts in reaching your crown jewels.

pentest
INFORMATION SECURITY ASSURANCE

The more sensitive the data the more authentication factors you may want to consider, and it's not uncommon for companies to employ three or even four factor authentication when it comes to extremely critical information.

> Employ a Virtual Private Network (VPN)

Access to sensitive servers and information should be restricted to internal networks only. However, if remote access over the internet is required, then this should only be provided via a VPN solution.

Requiring a VPN to access services will ultimately increase the protection around sensitive information and make it more difficult for attackers to access this information.

When employing a VPN solution, you'll need to ensure that it is appropriately encrypted and can only be authenticated using multi-factor authentication.

Encrypt your data

Strong encryption should be used wherever possible and will help prevent unauthorised access to your critical information.

Any data in-transit, i.e. traveling over a network, should be appropriately encrypted and the SSL/TLS suite is the most popular solution to this problem. If this is used, then you need to ensure that only recent versions of the protocols are in use and only strong cipher suites are utilised.

Any sensitive data at-rest should also be encrypted. The most common example of this is insisting on full-disk encryption for corporate laptops.

Harden your configuration

Modern operating systems are fairly secure straight out of the box; however, security improvements can always be made. This is often the same for many technologies.

Hardening the configuration of your technology means you safeguard your systems against the latest cyber threats and hardening guides, such as the CIS Benchmarks, can provide helpful guidelines on everything from operating systems and server software, through to network devices and desktop software.

Employ a robust patching process

Have you ever clicked the ‘remind me later’ button when asked to update your software or operating system? Of course you have, we all have, we’re all busy people and we don’t often feel we have the time, or energy, to restart systems whilst trying to go about our daily lives.

But updates are important. Not only do they provide new features, they provide critical security patches. Patches which help protect you against cyber-attack.

Any delay in updating can increase the likelihood of a successful attack and it’s often a race against time before malicious threats uncover the previous vulnerability and weaponise it.

A robust patching schedule is therefore vital and you should be ensuring that you’re scheduling business wide updates on a regular basis.

Build defence in depth

Putting up defences around your crown jewels is obviously key, but are you putting up defences throughout your business?

Defending a network should be like defending a castle, if an attacker gets through one set of defences there should be another set waiting for them. This is called defence in depth and the more effective defences you have in place throughout the business, the more difficult you make it for attackers to gain access.

step 3: put your defences to the test and fix the issues you uncover

As we mentioned in step 2; the more effective defensive measures you put in place, the more difficult you make it for would be attackers.

But how do you know if your information security defences are truly effective?

You need to test them.

Having your work tested can seem like a daunting prospect and it can be easy to think that it’s going to belittle or ridicule your security efforts. But that’s not the case. Testing is here to support your efforts, ensuring that your business is as protected as it can be and allowing you to make informed decisions about your next steps.

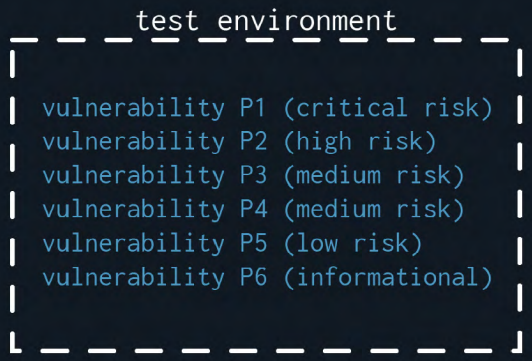
But what types of information security testing are available?

Penetration testing

Penetration testing looks to uncover as many potential vulnerabilities as possible within a clearly defined test environment, and within a set time period. This test environment could be a web application such as a website, a mobile application, your internal infrastructure, production systems, cloud services, embedded devices or your even wireless networks. Remember, it's always best to start with your company's most critical assets.

The vulnerabilities uncovered are categorised according to the risk associated and a final report should give you the remediation advice to allow you to prioritise your future security improvement efforts.

Whilst penetration testing can uncover many vulnerabilities, it can only outline how those vulnerabilities could potentially be used as part of a wider attack chain and consultants can only advise of further attack chains based on previous experience and/or theory.



Red teaming

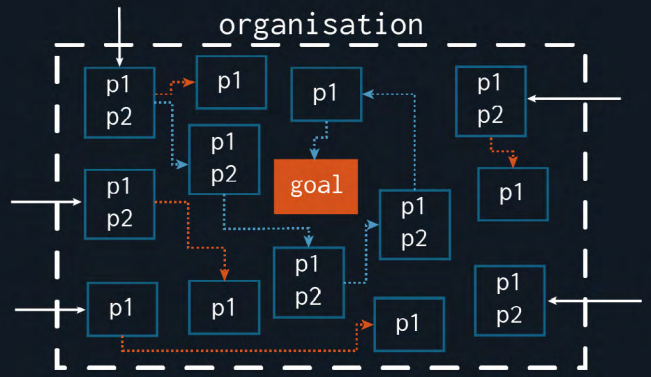
Red teaming is designed to simulate the actions of a real cyber-attack against your business.

Unlike penetration testing, red teaming is goal based and consultants will utilise any route possible, within the set scope, to gain access to a privilege level or set of resources that could be highly impactful to a business.

This testing isn't about finding all vulnerabilities present within a business, just the ones that can be exploited to achieve the set goal.

Essentially, red teaming allows you to find out if an attacker can gain access to your crown jewels and what routes they would take.

Again, remediation advice should be presented in a final report, allowing you to make the necessary fixes to stop attackers utilising any routes uncovered.



Which one should you choose?

In an ideal world both types of testing should be utilised, but in very different ways.

If you have never conducted any information security testing before, or conducted very little, then penetration testing should always be your first choice. This type of testing will allow you to uncover as many vulnerabilities as possible, within key areas of your buisness, allowing you to fix issues and help start to build up your company's wider defences over time.

Red teaming is used less frequently and is ideal for those that have already conducted some previous penetration testing or feel their defences are able to be put to a wider test.

pentest
INFORMATION SECURITY ASSURANCE

step 4: don't let security be a one-off exercise

Information security can sometimes be seen as a tick box exercise and there is often a belief that a one off, annual security assessment is enough to keep a company protected until it's time to test again next year.

This isn't the case and just because you've been tested today doesn't guarantee you won't get breached tomorrow.

Attackers are always looking for new attack routes and no company, or technology, is 'unhackable'. Given enough time, information, resources and dedication, attackers can always find a route in.

Security improvement efforts therefore need to be ongoing, helping keep your company one step ahead of these malicious threats.

So, remember:

> identify your crown jewels
> protect them
> test your defences and fix the issues
> start your security efforts again

pentest
INFORMATION SECURITY ASSURANCE

supporting your information security improvement efforts

Pentest Limited is a leading provider of penetration testing, red teaming and offensive information security consultancy services across the UK, Europe, USA and Asia.

We pride ourselves on our client-focused approach and our services are designed to not only uncover IT security vulnerabilities but to support your ongoing information security efforts, to pass on our wealth of expertise & to increase the digital resilience of your business.

We work with companies of all sizes, and whatever your goal, we're here to support you. It's this support that truly sets us apart and our team will be on hand throughout engagements to impart their expert knowledge, deliver industry best practice and provide you with vital post-test remediation advice.

Find out how we can support your information security efforts by visiting www.pentest.co.uk, call us on +44 (0)161 233 0100 or email us via contact@pentest.co.uk