Assess your network's vulnerabilities before a malicious threat actor gets to you.

Cyber security on your mind but can't make a concrete decision on which services might be right for your business?

Businesses can opt to start from either getting a Penetration Testing (pen testing) service performed or risk assessment done to assess their cyber security posture. Pen testing involves assessing your network and web applications for any vulnerabilities that could be exploited by malicious actors. It's essential to identify these weaknesses before an attack occurs, so right measures can be taken to protect your data and systems.

Continue reading to explore why a penetration test is probably one of the smartest precautions you can take to protect your company from attack ⟶

Identify Weaknesses in Your Network Security

Penetration tests is essentially hacking but in an ethical way. These tests are designed to simulate real-world attacks using the same methods attackers use when attempting to breach a system. This will allow you to identify any weaknesses in the current security posture which could be exploited by malicious actors, allowing you time to patch those vulnerabilities before an attack occurs. Additionally, penetration tests can help with the tools and tactics attackers are likely to use during an attack so that you are better prepared for future attempts.

Gain Insight Into Your Organisation's Security Posture

One of the key benefits of performing regular penetration testing is having insight into how secure your organisation really is. It will allow your IT/Security team to get an accurate picture of where the organisation stands in terms of its ability to detect and respond to threats quickly and effectively.

By gaining this insight into the organisation's security posture, it helps to understand where the strengths lie and where improvements are needed in order for the business's security posture to remain up-to-date with ever-evolving threats.

Highlights

- Is your business safe from hackers? A penetration test is probably one of the smartest precautions you can take to protect your company from attack.
- New Zealand's top business leaders say there are wide and growing gaps in cybersecurity, with the day-to-day operations of the country's largest companies and SMEs constantly in the crosshairs.
- One of the key benefits of penetration testing is allowing your IT/Security team to get an accurate picture of where the organisation stands in terms of its ability to detect and respond to threats quickly and effectively.
- Your customer's privacy should be your highest priority and placing appropriate technical and operational measures will show the stakeholders that you are serious about protecting customer data and ensuring the security of your network.

Showcase security commitment to your stakeholders

Pen testing isn't a one time solution. By conducting regular penetration tests, you can show the stakeholders that you are serious about protecting customer data and ensuring the security of your network. This helps to build trust with customers and partners, as well as demonstrate a commitment to upholding the highest security standards.

Prioritise efforts on high severity vulnerabilities

Penetration tests can help you prioritise your security efforts by highlighting the most critical vulnerabilities that need to be addressed first. This allows teams to quickly identify and patch any high-severity issues before they become an even bigger problem.

Growing gaps in NZ's cybersecurity

New Zealand's top business leaders say there are wide and growing gaps in cybersecurity, with the day-to-day operations of the country's largest companies and SMEs constantly in the crosshairs.
Key findings show:

- One in three (36%) businesses impacted by cyber-attacks or incidents say their business operations were disrupted
- 28% of businesses impacted by a cyber-attack or incident point to third-party suppliers as the cause
- 70% of business leaders say they would consider paying a ransom to a cybercriminal
- Cloud misconfigurations or software vulnerabilities were responsible for causing cyber incidents for almost two out of five (39%) businesses
- Around 46% of cyber incidents and attacks took longer than one month to resolve
- 29% of businesses suffering a cyber incident say personal data was stolen or accessed.

AMARU is a CREST-certified pen testing partner for businesses across Australia & New Zealand.

We are the consultants your business needs to help you gain insights on your network's vulnerabilities and offer reliable solutions to strengthen your security measures.

Skilled team of professionals: We specialise in pen testing and our team consists of CREST-certified pen testers with OSCP, OSEP, OSWE, CPTC, eWPT.

We care about your business like its ours!
We go above and beyond to provide you with the highest level of protection and support throughout the process, just like we would for our own company.

Working with the best across industries

NETVALUE BETTER BUSINESS · Spectrum care · Figured · Harmoney · HYUNDAI NEW ZEALAND · FIJI AIRWAYS · SolarZero · eventfinda · APEX · optimation · Cone Marshall · ember KOROWAI TAKITINI

About AMARU

AMARU is ANZ's leading information security and compliance service provider, offering end-to-end managed cyber security services across Australia, New Zealand and Fiji.

www.amaru.co.nz hello@amaru.co.nz