CASE STUDY:
Red Piranha and Oz Snow

Red Piranha

I would highly recommend Red Piranha. We were completely blind to some major issues that would not have been remediated without the help of RP. Their customer support has been fantastic, and I have always been able to get any help that I require within one phone call. I sleep much easier having these guys taking care of our data security"

– Nick Marko – IT Manager at Oz Snow

OZ SNOW
ozsnow.com

Background

Australia's Oz Snow has been committed to offering affordable, quality snow trips to skiers and boarders since 1999, providing packages to both individuals and groups including Corporate, University, Schools, and Community Groups.

Oz Snow is an all in one accredited tour operator, travel agent, hotel and lodge owner. This approach enables them to have greater control and organisation of their tours while keeping prices down, with better facilities and services to cater to their customers' needs.

Challenge

Being an organisation with a global presence and being a continuous target, Oz Snow understood the risks they faced daily.

To establish their current level of exposure and meet compliance, Oz Snow engaged the Security Team at Red Piranha to conduct a Penetration Test to learn more about their vulnerabilities and how they can be addressed.

Additionally, they had specific business continuity and compliance requirements, relating to its duty of care to maintain employees' and clients personal and financial data. With an international presence, the penetration test itself was needed to be conducted on multiple assets and targets globally to ensure the highest level of coverage and assurance.

Solution

Red Piranha conducted extensive penetration testing on all of Oz Snow's cloud applications, websites and portals and found Oz Snow was exposed to several high-risk vulnerabilities. Red Piranha provided a detailed report of all the areas that required immediate attention, listing all the vulnerabilities with the level of risk and examples of how those vulnerabilities could be exploited.

Red Piranha's Security team performed an analysis of the information from public resources, completed a vulnerability assessment to discover all vulnerabilities in the target web and application servers and the carried out two types of manual security penetration tests;

- Blind penetration testing; to simulate real-life hacking
- Controlled hacking of the target systems by experts certified in information security to confirm and identify both known and undetected vulnerabilities

Result

Following the completion of Red Piranha's testing services, Oz snow was provided with a comprehensive report detailing the list of discovered vulnerabilities and configuration weaknesses which could be exploited, countermeasures and recommendations from the blind penetration testing.

Oz Snow's management team also participated in training on the existing information security risks the organisation faced and is continuing to work with Red Piranha utilising their vCISO (Virtual Chief Information Security Officer) service, currently being used to attain their ISO 27001 certification and PCI compliance.

Crystal Eye UTM appliances have also since been deployed to secure the organisation's network from Cyber Threats.