BIZCOMMUNITY

How ethical hacking can improve your security posture

By Prabashni Naidoo

23 Jan 2020

Cybersecurity professionals see some threat actors or outside-parties as the enemy. However, challenging this mindset is important; you can better protect your organisation against outside-parties if you understand how they think and operate.

Prabashni Naidoo, director at Amazon Web Services South Africa

With this in mind, businesses around the globe have turned to hackers to test security infrastructure and develop stronger, more robust security practices.

Before integrating penetration testing into your security policy, it is important to understand the different types of hackers that exist. Each group has differing motivations, and you must be clear on which of their skills can be used to your organisation's advantage.

Black hat

Black hat hackers are cybercriminals motivated by personal or financial gain. They range from teenage amateurs to experienced individuals or teams with a specific remit. However, over recent years, several high profile blackhat hackers have refocused on using their cyber skills to protect organisations.

An example is Kevin Mitnick aka Condor, who was just 16-years-old when he gained access to a Department of Defense computer. Following this and numerous other hacks, Mitnick spent five and a half years in prison. Upon his release set up his own company, Mitnick Security Consulting, which now runs penetration tests for clients.

The issue of whether to work with a previous black hat hacker is a contentious one. Some, including David Warburton, senior threat evangelist at F5 Networks, believes that hiring ex-hackers is critical in staying ahead of the threat landscape.

However, others are concerned about allowing this group access to corporate systems and customer data. The latter group should, however, consider other approaches to working with hackers.

White hat

Often referred to as ethical hackers, white hat hackers are employed by organisations to look for vulnerabilities in security defences. Despite using the same tactics as black hat hackers, this group has permission from the organisation making what they do entirely legal. While they use their knowledge to find ways to break the defences, they then work alongside security teams to fix issues before others discover them.

Many of the biggest organisations in the world, including General Motors and Starbucks, are turning to white hat hackers to help identify fault lines and proactively enhance security posture. White hat hacking can offer an interesting and lucrative career path for people with technical skills. Drawing attention to the important role white hat hackers play can encourage more talented individuals to take a positive path instead of becoming black hat hackers.

Nurturing talent

There are many programmes in place to find, encourage and support the next generation of white hat hackers. An example, supported by AWS, is r00tz Asylum, a conference dedicated to teaching young people how to become white-hats. Attendees learn how hackers operate and how cybersecurity experts defend against hackers. The aim is to encourage people with technical expertise to use it for good in their career.

By equipping aspiring cybersecurity professionals with knowledge and skills, they can bake security into infrastructure, from the ground up. AWS's support for r00tz is our chance to give back to the next generation, providing young people who are interested in security with a safe learning environment and access to mentors.

Building on solid foundations

For those responsible for maintaining customer trust and protecting data, an end to end approach to security is critical. As we have seen, working with ethical hackers is a powerful way to view security posture from a cyber-criminal's perspective to identify and tackle vulnerabilities.

However, it's also important to remember that security needs to be baked in throughout an organisation's infrastructure. This is where partnering with a cloud platform can be beneficial; the best of these are developed to satisfy the needs of the most risk-sensitive organisations. Cloud platforms also offer automated security services, which can proactively manage security assessments, threat detection, and policy management.

In so doing, these platforms take on a lot of the heavy lifting for security professionals, including ethical hackers.

ABOUT THE AUTHOR

Prabashni Naidoo, director at Amazon Web Services South Africa