Why businesses should prioritise application security

By Glenn Morgan

5 Jan 2021

Application development is becoming an important business differentiator as companies embark on a digital transformation. Yet, many organisations treat cybersecurity as an afterthought - and this oversight leaves applications vulnerable to attack.

Glenn Morgan | image supplied

According to *Security Magazine*, an online attack occurs every 36 seconds, with these numbers likely to increase as the internet is used by more businesses and people.

Applications are the front layer to critical data, and that's why there's been an exponential rise in hackers attacking applications to access this data. Application security, therefore, is increasing in importance and should be a top priority for any modern business looking to protect its assets.

Designing apps for both internal use and to bridge the gap between consumer and company is often a major security risk for businesses as they potentially open themselves up to attack. It becomes much harder to combat these potential breaches as developers are pushed to deliver feature-rich applications in shorter periods of time, often overlooking security best practices.

Continually testing established systems and future installations is also a requirement as new threats are developed every day. Roughly 317 million new forms of malware are created every year, and businesses need to be prepared for them.

Where possible, businesses should be actively involved with the development and installation of applications so they can continually check for and monitor potential security threats. These can then be dealt with in a timely fashion.

What does application security involve?

Essentially, application security involves adding features or functions to software to find, fix, and avert vulnerabilities that could result in cyberattacks or data breaches.

When implementing application security protocols, there are certain requirements that must be met. Rushed development and installation can often lead to glaring gaps in a business's online security, with many nuanced faculties often being overlooked. Many organisations find that the best way for a company to oversee the process is through the assistance of a trusted ICT partner that can offer professional guidance.

Sometimes, businesses see application security as a box that just needs to be ticked, and many hurry to implement security solutions without actually ensuring they're automated or measure up to industry standards. This is the wrong approach; effective security requires security considerations to be baked into every step of the development lifecycle.

Future-proofing your application security

The countermeasures implemented to protect an application or system should be designed as widely as possible, rather than trying to home in on specific threats. It's important to remember that application security must cater to a next-generation era of IT as well as the present.

Manually testing for all these potential threats is impossible. Instead, this requires the implementation of an optimised automated system. The application of these defensive measures needs to be as seamless as possible to ensure that users are responsive to potential system changes and aren't required to drastically alter how they interact with the application itself.

With businesses constantly engaged in online evolution, a comprehensive strategy is required to counter potential threats. Effective monitoring for possible attacks, a secured pipeline, and detailed feedback on system infrastructure will pay for itself in the long run.

Finding the right partner

An effective cybersecurity plan is arguably one of the most important investments a modern business can make, especially if it's planning on embarking on a digital transformation journey. We've seen this more and more recently, with several prominent brands in the news for data breaches. Most businesses recognise the benefit of having secure applications, but it's just not in their set of core business skills.

DevSecOps is not something that is simply 'turned on' within an organisation. It involves aligning the people, processes, and tools that are involved in the development lifecycle. The right ICT security partner should be able to consult on application security aspects as well as assist in reviewing and consolidating all the tools and processes in the chain.

Look for a partner that understands vulnerability management and has a broad security knowledge base on ICT security, not just experience with DevSecOps.

Not all older technologies are suited to this new way of working, and in some instances, it may be necessary to make recommendations on toolsets that could be better suited to securing newer environments, like cloud platforms and containers. This approach will enhance the overall security and compliance posture of the pipeline.

With the right partner, application security doesn’t have to be a challenge, but rather a way to ensure that your business survives and thrives in an often-hostile online environment.

ABOUT THE AUTHOR

Glenn is a security pre-sales consultant at Puleng Technologies.