Find your vulnerabilities before your attackers do.

The internet is still very much the wild west, where malicious individuals and ‘state-sponsored actors’ can cripple your business and hijack your data with a few well-executed keystrokes. Whether it is financial information, system passwords, or intellectual property, a data breach can expose your business to an incredible amount of risk.

Your information and that of your customers must be kept private. Your reputation and your bottom line depend on it.

There are so many ways your security can fail, making the task of finding vulnerabilities during testing that much more critical. Which is why it’s crucial to test your security with our highly experienced security professionals.

With spriteCloud, you are in safe hands. We’re the experts at uncovering vulnerabilities, and we handle your information with the utmost discretion and confidentiality.

Penetration Testing Services

- Web application penetration testing
- Infrastructure penetration testing
- Mobile application penetration testing

spriteCloud

Web application penetration testing

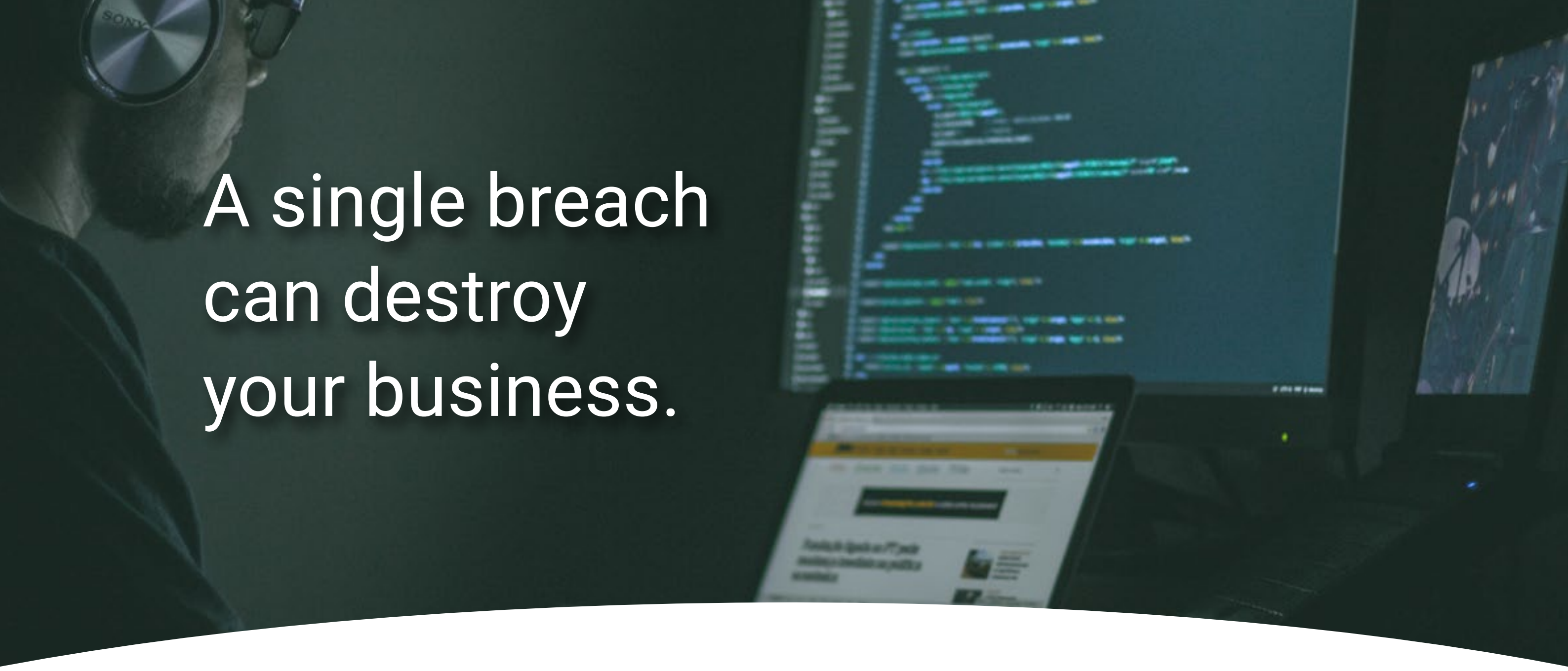
A web application penetration test uses manual and automated approaches to identify security threats or vulnerabilities in your web application. The purpose of these tests is to determine possible threats and identify ways to mitigate them across the whole application and its components (database, source code, back-end services). Our team of OSCE and OSCP certified ‘ethical hackers’ use exploits (like SQL injections and XML External Entity (XXE) injections) to constantly probe ways to gain control of your web application; so that you can prevent others from doing so.

We offer three approaches to web application penetration testing.

Black-box
The tester is placed in the shoes of a normal internet user with no knowledge of the how the application works or access to its source code. This method is closest to what a real hacker would face when trying to penetrate your application.

Grey-box *(most common request)*
A combination of black and clear box testing, testers can create exhaustive tests while remaining close to realistic attack conditions. Testers are given knowledge of the internal workings and functionalities of the applications but without access to the source code. Testers use their knowledge of the system to test the application more thoroughly.

Clear-box
This testing approach requires the tester to have access to the source code of the application. This allows the tester to check the quality of the code, within a larger scope normally provided by a developer. While not representative of real-life conditions, it does allow for the more effective securing of applications.



A single breach can destroy your business.

Infrastructure penetration testing

With multiple computer systems, devices and users, your infrastructure has many points through which malicious actors can gain entry and wreak havoc. Our infrastructure penetration testing gives you a head start by helping you plug gaps in your defences and ensure that your customer data, intellectual property and financial information remains secure from threats, both external and internal. Our certified security experts are trained to help you turn your network into a virtual fortress.

We offer two approaches to infrastructure penetration testing. These methods are 'black box' external infrastructure testing and internal infrastructure testing.

External infrastructure testing

Exposures due to weak firewall configurations, flaws in application code or patch issues can leave you open to attackers gaining entry to your system. An external infrastructure penetration test helps identify these possible points of entry and provides an assessment as to how they can be secured. This method is meant to replicate how an attacker, with no knowledge of the system, would approach your infrastructure.

Internal infrastructure testing

An internal pentest looks for security issues within your network. A compartmentalised networks ensure that disgruntled employees or attackers that have gained access to your internal network are mitigated. These internal network attacks can be extremely costly and disastrous for businesses and their reputations.

> "Your information and that of your customers must be kept private. Your reputation and your bottom line depend on it."

Mobile application penetration testing

Just as quickly as mobile devices and mobile applications have become a part of daily life, so too have security breaches and attacks increased in frequency. A major cause of this is the increased time pressures that developers face to provide new functionalities and bring the apps to market.

All these reasons make frequent mobile application penetration testing crucial in order to protect the reputation of your app and your business. Our team of security experts will help you uncover vulnerabilities and secure them.

Are your applications and systems secure? Now is the time to find out, before an attacker does.

Contact spriteCloud for more information.

Call us at +31 (0) 20 61 59 155 or email at info@spritecloud.com