CASE STUDY

Preventing Crises

In a world in which uncertainty is on the rise and new risks are regularly emerging, even a single event may threaten the future of an organization. What would you do to prevent an event?

Trustwave®

Client Spotlight

This Trustwave client is a private crisis management solutions provider. More than 750 global brands leverage its platform to prepare for and respond to a broad array of traditional and digital crises, from product malfunctions to food poisonings.

The Challenge

The client's product, a mobile application, provides instant access to a crisis plan for the team inside an organization who is called to respond when an emergency strikes. Those managing the app can provide real-time updates and notifications to the rest of the organization with a simple push of a button.

Imagine one of the top U.S. banks in a time of crisis. Now imagine if the app they leveraged to communicate with employees and customers during that time of emergency was compromised by cybercriminals. How much additional damage could they cause? As the provider of such a cloud-based application, the client required a product that could generate trust for Fortune 100 brands.

Familiar with following strict DoD Directive 5000 series instructions, the management team of the client was looking for a company that could test the resiliency of its application, through a mobile security assessment that would involve vulnerability scanning and penetration testing. Plus, it needed to perform this assessment within budget parameters.

> *"As a small, 25-plus employee company, we can't afford independent third-party tests more than once a year. Having access to the Trustwave Security Testing Suite platform really helps us save money and time. We catch vulnerabilities and mitigate risks faster."*
>
> – Chief Technology Officer

The Solution

Trustwave helps the client meet its business objectives efficiently through our Security Testing Suite. Throughout the year, the client buys credits that go toward testing hours completed by Trustwave ethical hackers, who are part of the elite SpiderLabs team at Trustwave. Within the Trustwave platform, the client chooses its preferred level of intensity for the the simulated attack, schedules a time for the test, and provides access credentials and any directions Then, the Trustwave penetration tester takes over, leveraging global intelligence data to mimic the activities of a malicious hacker trying to break into the app.

> *"Trustwave has a very good name in the industry, which gives me confidence when talking to clients."*

Before the SpiderLabs team stepped in, the client applied security patches only once a year. Now, its software development process can constantly integrate security patches within every agile release, maintaining focus on the rapid delivery of business value.

The combination of annual vulnerability testing and penetration testing, as part of a managed security service, provides the client's CTO with proof that its application is secure. The internal IT workforce (can now concentrate on more strategic projects, and its developers have the performance metrics they need. The company's customers have confidence that the application will be available if and when a crisis should occur.

Industry Threat

Due to the proliferation of mobile apps, users have become accustomed to agreeing to system permissions without checking the security and privacy risk that comes goes along with it. Many apps today store personal and corporate data in remote servers – in some instances in the cloud – that hackers could compromise.

Trustwave®

CS-CRisisMgmt-0519