terreActive
terreActive
terreActive
terreActive

Penetration testing for a web application. Trust, but verify.

Build greater trust by having an independent third party validate security.

How can a company demonstrate that it's keeping its promise to ensure data security? Penetration testing performed by an independent body delivers clear results. In the case of LegacyNotes, the service provider for digital estate planning, it has shown that customer data is in good hands.

The data that LegacyNotes has stored couldn't be any more personal: customer information in the form of data related to retirement planning and estates, such as health care proxies and living wills, bank accounts and insurance policies, social networks or even funeral requests.

All of these estate-related details and instructions are encrypted in a secure, central location, are retrievable, can be accessed at any time and from anywhere, and can be changed if necessary. They can be shared specifically with relatives and other trusted individuals – either immediately or only after the data subject's death.

Helpful hackers at work

The procedure and scope of the tests to be deployed for the publicly accessible web application were defined at a joint kick-off meeting. The subsequent penetration attempts aimed to detect and identify potential vulnerabilities in the system. The fact that both potential external attackers and individuals who have an existing relationship with customers try to gain unauthorized access to other people's data was taken into account. LegacyNotes was continuously informed of how the project was progressing.

While the tests were being carried out, the results of all the steps of the investigation were analyzed and documented in an audit report.

An audit to ensure transparency and security

Once the tests were complete, the audit report was sent to the client in preparation for the final meeting, where the project and the results achieved were presented and questions clarified. The project was concluded with recommended measures for eliminating risks.

"The terreActive pentest confirms our key customer promise: 'We offer you the data security we'd like our own data to have on LegacyNotes.'" said Thomas Jaggi, co-founder and CEO of LegacyNotes.

Cybercrime is steadily increasing, and the methods used are becoming more and more sophisticated. Sensitive customer data is a valuable asset that we are entrusted with, and it mustn't fall into the wrong hands, which is why it's advisable to schedule regularly recurring audits, especially for web applications that can be accessed externally. This allows vulnerabilities to be identified in a structured manner and to be continuously eliminated.

"terreActive's long-standing business relationships involving the handling of highly sensitive data from banks, authorities and insurance companies gave us the confidence that we were relying on the right partner for the auditing process."

Thomas Jaggi, CEO

LegacyNotes

A good feeling

Penetration tests are an efficient tool for examining applications' security and questioning the status quo. LegacyNotes can now rest assured that the right decisions have been made – both in terms of the basic architecture and the technical implementation.

This is an important indicator for customers. Promising security is simple; actually delivering it is demanding.

Additional benefits

- During the penetration test, other security-related questions concerning the access rules for customers and their appointed proxies were clarified too.
- Another positive consequence of an audit or a penetration test is that employees become more aware of security.
- Online payment must remain embedded as close to the application as possible to dispel any doubts about its trustworthiness. But at the same time, it must be well-isolated to prevent attacks through the payment service provider. Various ways of implementing this requirement were discussed at the end of the project.

The penetration test procedure

ASVS (Application Security Verification Standard) according to OWASP (Open Web Application Security Project).

The ASVS is a collection of established best practices for securely implementing web applications. In the scope of the investigation, the review categorizes the implementation of best practices into:

- Met or not met.
- Not applicable, e. g. if the feature to be tested doesn't exist.
- Not testable, e. g. if individual topics were excluded from the scope of testing from the outset.

LegacyNotes

is the personal, secure and independent companion for digital estate planning. LegacyNotes simplifies the administrative work and supports your loved ones when you're no longer able to do so yourself. You can easily manage your estate, back up important data and determine how your digital accounts are handled.

Our vision:
Nobody should to leave this world without having settled everything for their loved ones.

www.legacynotes.ch

Audits and ASVS best practice

The following is an excerpt of a potential presentation of the degree of fulfillment. This example is detached of the project described here.

ID	ASVS best practice	Rating
P1	The application has sufficient anti-automation checks to identify and prevent data exfiltration, excessive use of functions, excessive file uploads or denial-of-service attacks.	High
P2	The application does not disclose internal information about the infrastructure or components.	Medium
P3	Ensuring that a content security policy is in place to minimize the impact of XSS attacks.	Medium
...	...	...