Deloitte. SECURITY SCAN

TOOLS4EVER
IDENTITY GOVERNANCE & ADMINISTRATION

Another Successful HelloID Security Scan!

Twice a year, Deloitte experts test the security of our HelloID service. The recent test proved again that the HelloID security is at a very high level, but what does this mean? Let us look closer at why Deloitte's ethical hackers conduct this test.

For Tools4ever, this is always an important test. It keeps our experts sharp and stimulates the ongoing improvement of our technology and services. For you as a customer, it is important to know independent specialists test the HelloID solution every 6 months with a critical eye to discover any vulnerabilities before they can lead to any harm.

WHY A SECURITY TEST BY EXTERNAL 'ETHICAL HACKERS'?

Needless to say that as a company developing Identity & Access Management products, we have a large number of security experts within our own ranks. And of course, we frequently ask our experts to try to attack our own solutions. Nevertheless, we think it is important that there is also a regular evaluation of our systems by external experts. Such external tests prevent the occurrence of blind spots and assist us with an extra pair of eyes.

By choosing the ethical hackers of Deloitte, we have opted for guaranteed independent and highly qualified security experts. It is crucial to us that Deloitte verifies the integrity of all its experts, so that you as a customer can be sure that the test results are not misused in any way.

SCOPE OF THE HELLOID SECURITY TEST

The biannual survey is not a 'paper tiger'. It is not just a desk review of the HelloID design and specifications. The test consists of a large number of attempts by professional ethical hackers to attack the HelloID solution. These ethical hackers have been trained to look at IT systems from the point of view of an experienced cybercriminal to recognize vulnerabilities that others might overlook. They use for example the NCSC ICT-B v2 guidelines and the OWASP Top 10 Application Security Risks of 2013 and 2017.

The test procedure naturally includes the traditional black box tests. Such tests are aimed at getting unauthorized access to functionality and data without knowledge of the system. However, in our application security tests, the testers go further and execute also so-called grey box tests. A grey box test looks for security weaknesses in specific parts of HelloID, using inside information about the design and operation of the software. Finally, we look at the possibilities for authorized users within the system. Do they have 'unintended' possibilities which go beyond what's necessary for their role? The industry has known for a long time that fraud and cybercrime often take place from within organizations. So, at HelloID, we not only test the quality of our 'front door', but also look at the security of the application against someone authorized to use it.

The tests themselves cover the full range of potential vulnerabilities: from system reports providing too much details, to the presence of cross-site scripting (XSS) vulnerabilities.

RISK ANALYSIS

Every potential vulnerability that comes to light receives a risk qualification that helps us to tackle the problem with the right priority. Such a risk qualification depends on the chance that a potential vulnerability can be discovered and exploited, and the impact if this really happens:

- The chance depends, for example, on the complexity of the vulnerability in question. Is the vulnerability abused by following a simple step-by-step plan or is physical access to the servers necessary?
- The impact is defined by the potential damage that a vulnerability can cause. It obviously makes a big difference whether this is a short-term interruption of the service or a serious data leak.

The test report always lists the Low and Medium Risks, which our experts promptly get to work solving. High Risks are directly escalated by the test team so that Tools4ever experts can immediately develop and roll out a solution. Fortunately, such vulnerabilities are rare.

Low and Medium Risks unavoidably pop up on every test. The technology is constantly evolving, as well as the knowledge and tools available for cyber criminals. Therefore, our work is never finished and we always will find things to improve. Constantly targeting that improvement is the big added value of our 6-month security scan. We stay sharp and keep the HelloID service fully up-to-date in terms of security technology.

DO YOU WANT TO KNOW MORE ABOUT THE SECURITY SCAN?

Of course, we cannot publish the detailed contents of our security scans. However, you always see the effect in the form of adjustments, improvements and bug fixes in our regular release notes, and your account manager will gladly tell you more about our regular security tests.

Tools4ever
Amalialaan 126C
3743 KJ Baarn

tools4ever.com
sales@tools4ever.com
Tel: 035 54 255