

“It was definitely worthwhile for us. We found some things that we can improve. That’s why you hire an independent tester.”

Thomas Pedersen
Founder and CEO
OneLogin

OneLogin Builds Customer Trust with Rapid7 Application Penetration Testing

The rise of cloud applications complicates management and security of user accounts. “With everything moving to the cloud, the enterprise no longer has tight control over access to its data,” says Thomas Pedersen, founder and CEO of OneLogin. “Our customers typically use between 30 and 40 applications company-wide, and some use even more.”

Directory management, such as adding or deleting multiple cloud accounts as people join and leave a company, presents a significant burden to IT managers. OneLogin (www.onelogin.com) helps IT managers to regain much of the control they had when enterprises stored all their data behind the firewall. OneLogin lets users launch all their web apps from a single sign-on portal or from the company’s intranet – in one click. Users only have to remember one strong password—a simple, elegant solution for an increasingly complicated IT world.

Challenge

“In many cases, we store a lot of our customers’ company passwords in our database,” says Pedersen. “So the concern that some customers had is: ‘What happens to your database if your system gets hacked?’ Some criminal could access the passwords.”

While OneLogin takes appropriate measures to protect its network, Web, and database infrastructures during development and day-to-day management, Pedersen considered how to address these customer concerns. “It’s all about trust. Most of our customers are fine living on the strength of our passwords, but some of them need more assurance.”

Pedersen and his team decided to hire security consultants, who would attempt to penetrate OneLogin’s application logic, identify vulnerabilities, and recommend remediation as needed. “It’s an insurance policy for us. If we get hacked, and we get on the front page of a tech magazine, it’s definitely going to impact our business. It’s going to damage our reputation.”

Based on their own experience, a OneLogin customer recommended working with the Rapid7 Professional Services team, and Pedersen added Rapid7 to his short list of security specialists.

Solution: Rapid7 Network Penetration Testing

Rapid7 Professional Services is a full-service enterprise security assessment team. Rapid7 has conscientiously gathered a team of



About Rapid7

Rapid7 is the leading provider of unified vulnerability management and penetration testing solutions, delivering actionable intelligence about an organization's entire IT environment. Rapid7 offers the only integrated threat management solution that enables organizations to implement and maintain best practices and optimize their network security, Web application security and database security strategies.

Recognized as the fastest growing vulnerability management company in the U.S. by Inc. Magazine, Rapid7 helps leading organizations such as Liz Claiborne, the United States Postal Service, Carnegie Mellon University and Red Bull to mitigate risk and maintain compliance for regulations such as PCI, HIPAA, FISMA, SOX and NERC. Rapid7 also manages the Metasploit Project, the leading open-source penetration testing platform with the world's largest database of public, tested exploits. To obtain a free download of Nexpose or Metasploit, please visit <http://www.rapid7.com/resources/free-downloads.jsp>.

For more information, visit www.rapid7.com.

security experts with skills and areas of expertise that complement each other. They have an average of 10 years' enterprise security experience across a wide variety of industries from higher education to Fortune 100 companies. Rapid7 security consultants offer indispensable perspective on industry standards and coding practices and a deep, up-to-the minute knowledge of vulnerabilities, malware, and attack trends.

OneLogin asked the Rapid7 security consultant to perform a "black-box" network penetration test. Penetration testing is a method of probing and identifying security vulnerabilities in the network and pinpointing where a hacker can exploit an IT environment. The Rapid7 consultant would pose as a OneLogin user, and through a legitimate OneLogin account, attempt to access user information about other clients. The consultant used both advanced hacking techniques and the Rapid7 Nexpose vulnerability assessment tool to test operating systems, network devices, services, and database and Web application software.

The combination of white-hat guile and automated scans is the strongest strategy for proving the security of a system. OneLogin recognized that using a powerful tool such as Nexpose on its own, without the extensive experience of a consultant to interpret the results, might lead to an incomplete or distorted view of its true security posture. The consultant could differentiate results and prioritize vulnerabilities.

Results and Next Steps

The Rapid7 consultant presented a report to OneLogin that identified vulnerabilities, ranked them according to risk level, and included a prioritized remediation list. The OneLogin IT staff followed the remediation steps included in the report to plug the vulnerabilities.

"It was definitely worthwhile for us," says Pedersen. "We found some things that we can improve. That's why you hire an independent tester."

There is no such thing as perfect security. Hackers find new ways to penetrate systems every day and Rapid7 will perform ongoing network penetration testing to help OneLogin stay ahead of hackers.

It is important for OneLogin to be able to tell its customers that it is doing everything it can protect their confidential data. "It's peace of mind for our customers," he says, "And it's also peace of mind for us."