onelogin

FINAL REPORT
May 31st 2017 Incident

At OneLogin, we are committed to deliver on our promises. An ongoing promise we make to our customers is to be transparent, and we have not lost focus of that during every step of the May 31, 2017 incident. With that in mind, we wanted to provide an update on the security incident investigation and our remediation activities, which we initially shared with you back in June.

Our core values at OneLogin include Integrity, Urgency, and Customers for Life. This means that we are transparent with our customers and follow through on commitments. In the spirit of these values, we provide the following report on our review.

Root Cause Analysis

At this point, absent any unanticipated developments, our forensic review is complete and we do not anticipate learning additional details about the incident. We worked with outside cybersecurity experts to assess the incident and identify ways in which we could fortify our already robust systems and procedures. Our review, which included a third party forensic firm, included analysis of all relevant system, network, and AWS logs, as well as interviews with all relevant personnel. At this time we have no evidence of a technical vulnerability being exploited in order to gain access to our system.

Nevertheless, we focused our remediation efforts on preventive, detective, and corrective measures in areas that could have been targeted as part of this incident or might be targeted in future incidents. This type of exercise is not a one-time effort, but part of our ongoing risk management process that has been in place prior to the incident and which is audited several times a year.

AWS and SSH Key Management

The threat actor compromised a set of authorized AWS keys used to interact with our production infrastructure via the AWS API. To prevent that from happening again, we rolled out several enhanced procedures regarding AWS key management.

- AWS keys can only be used to generate short session tokens that are valid for a matter of hours
- AWS Management Console access and AWS API require a whitelisted IP and MFA
- More granular preventive and detective controls around high risk AWS functions

Additionally, SSH keys are generated by personnel without access to the Production Environment and stored within removable hardware authentication devices. The private keys cannot be exported or used without having access to the authentication device and are protected by an end user specific PIN that will trigger a lockout in case of a brute force attack. We also added hardware based MFA to the end user systems.

Network Hardening

OneLogin operates a cloud first environment for both our Corporate and Production Environments. In lieu of having on-prem systems, we leverage cloud service providers, similar to how our customers leverage OneLogin for their identity management. Therefore, the corporate network largely consists of Internet connectivity for our personnel. To further harden our corporate network, we deployed 802.1x authentication for the WiFi network, which uses our own OneLogin account for real-time authentication of end users. We have also rolled out DNS-based security monitoring for the TechOps team and end user system monitoring for high risk activities like connecting to public WiFi networks.

Data Encryption

OneLogin has always encrypted data elements like vaulted passwords and secure notes, and is now in the process of aggressively encrypting dozens of additional data elements throughout the system, because if it exists within OneLogin, that data is important to your company. This process is in progress and leveraging our new encryption service infrastructure.

Encryption Key Management

Each OneLogin customer has their own account encryption key that we use to encrypt their data. That key itself is stored encrypted using a master key we store outside of the database. We moved the master key to the AWS Key Management Service, which is backed by a Hardware Security Module and makes it more difficult to compromise the master key.

We have since deployed a distributed encryption service that handles encryption operations across all microservices. The main advantage here is that application code never touches encryption keys directly. Additionally, the centralized nature of the service makes it easier for us to rotate keys and monitor all activities related to encryption.

Bring Your Own Key

Now that we have moved key management to a centralized service, we are also able to offer customers to manage their own keys for additional control. We are in the process of implementing the infrastructure to support this and will be announcing the availability of Bring-Your-Own-Key in the near future.

Protecting Against Social Engineering

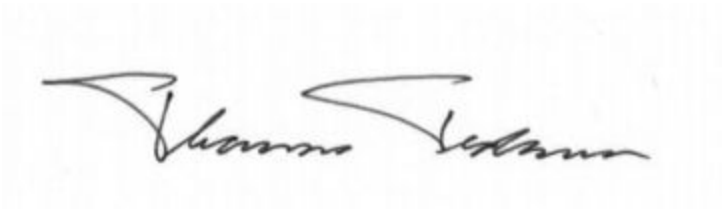
Our review has not revealed any evidence of social engineering, but it is still a risk all companies face. Over time, we have actively raised the security awareness of our personnel on this front by executing internal phishing campaigns and other exercises to gauge and improve the awareness of our personnel. We also are engaging a third party firm to perform a social engineering pen test against our company in order to further harden our overall security posture.

Delivering On Our Promises

While unfortunate, this incident made us stronger. When OneLogin had a two-hour outage in 2015, we knew this was completely unacceptable and that we had to make significant changes to prevent it from happening again. We moved from our co-location hosting provider to AWS and in the process changed our architecture to a highly distributed model that would protect end-users against any single point of failure. As a result, we now have the best uptime in our space and successfully weathered events in 2016 that took a heavy toll on many cloud services last year.

Similarly, we made, and continue to make, significant changes as outlined above in light of this incident. It is our firm belief that this incident resulted in a stronger and more secure OneLogin and that is a promise we know we can deliver on.

Sincerely,



Thomas Pedersen
Founder and Chief Technology Officer