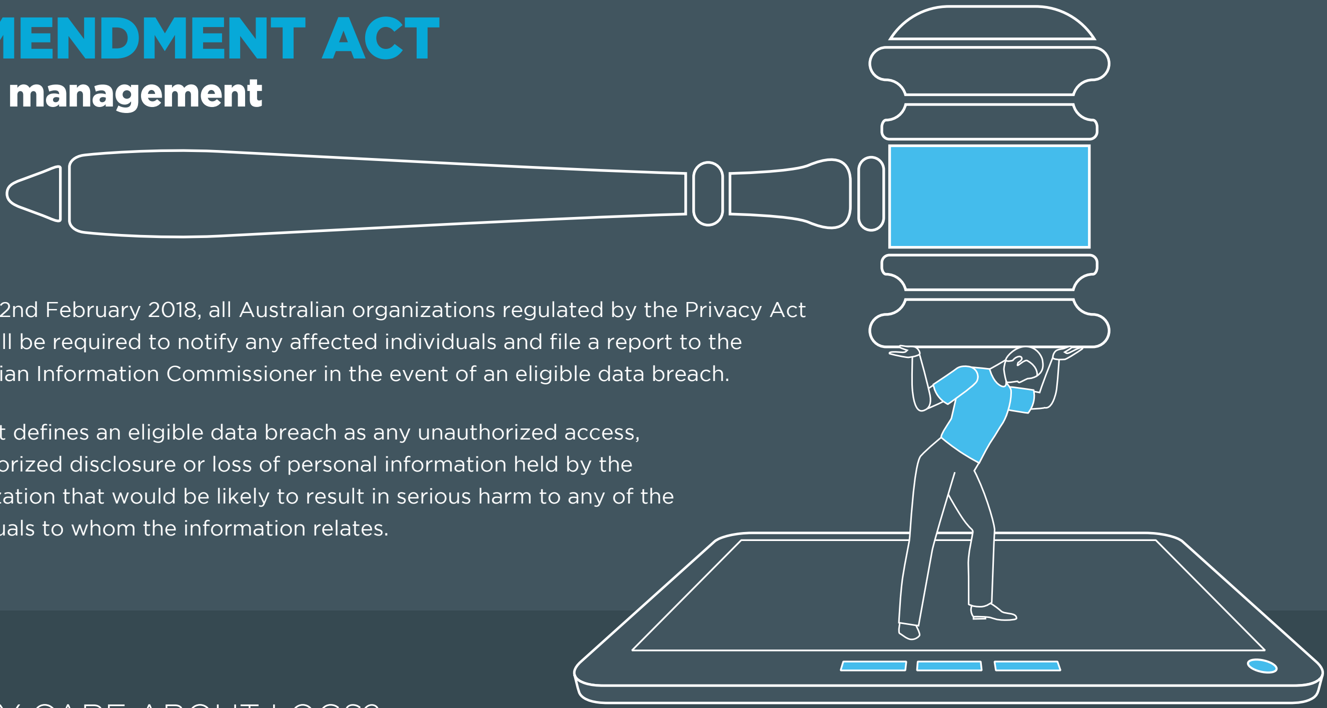
Data breach prevention aligned with the

AUSTRALIAN PRIVACY AMENDMENT ACT

Log management



From 22nd February 2018, all Australian organizations regulated by the Privacy Act 1988 will be required to notify any affected individuals and file a report to the Australian Information Commissioner in the event of an eligible data breach.

The Act defines an eligible data breach as any unauthorized access, unauthorized disclosure or loss of personal information held by the organization that would be likely to result in serious harm to any of the individuals to whom the information relates.

WHY CARE ABOUT LOGS?

Log messages play a significant role in all IT environments. Logs serve as a data source for security, threat detection, forensics, operations, debugging and business analytics purposes. At the same time logs are filled with personal information that require proper security in order to comply with the Privacy Amendment Act 2017.

Central log management is key to ensure personal information security and mitigating the probability of eligible breaches. To do so, logs must be secured at all time, both in motion and at rest.

WHAT ARE THE RISKS OF NOT HAVING CENTRAL LOG MANAGEMENT?

Distributed in silos

Without central management, logs are stored in separate data silos, making it difficult to have a clear overall understanding of their amount and content. This can make log related tasks tedious and inefficient, overall resulting in wasted resources and lower quality data for further decision making.

Filled with personal information

Logs function as a means of securing business critical assets in the network and at the same time they are filled with personal information content. This means that logs should be accessible only by those with explicit needs, and logs also should be protected during their entire lifespan.

Easily lost or corrupted

As logs arrive in tremendous amounts from multiple sources and in multiple formats, there is no denying that if your infrastructure is not equipped with failsafe measures, these logs can easily get lost or be corrupted due to stability, performance and processing issues.

ONE IDENTITY™

syslog-ng.com

HOW TO MINIMIZE THE IMPACT OF ELIGIBLE DATA BREACHES WITH LOG MANAGEMENT?

1 Securing logs from unauthorized access and unauthorized disclosure

SECURE TRANSFER

Log messages may contain sensitive information that should not be accessed by unauthorized users. This can be ensured by encrypting the communication channels between log sources and log storage facilities. Mitigating the probability of anyone listening in to the communication or to decipher any logs captured in transit.

SECURE LOG STORAGE

Once logs reach the central log storage, it is fundamental to encrypt their content to prevent unauthorized access. On top of that, adding time-stamping and signing will reveal if anyone tampers with the logs' content.

MASKING AND ANONYMIZING PERSONAL INFORMATION

To make sure that personal information in logs is secure all the time on top of the encryption process all personal information content can be masked by replacing them with hashes. Making only the necessary parts readable while keeping personal information safe.

2 Preventing message loss with secured transfer

DISK-BASED BUFFERING

If the log source is unable to connect to the central log server, logs can be stored on the local hard drive till the connection is back on.

APPLICATION LEVEL ACKNOWLEDGEMENT

In case of a connection loss between the client and the server, the client is capable of recognizing the last sent log to the host. Once the connection is back on, the client starts resending messages from that point, making sure messages are not lost or duplicated at the receiving end.

Conclusion

The Australian Amendment Act 2017 is a further indication of the importance of personal information security. Organization must have full understanding of their assets containing personal information. Log messages are one of those assets.

About One Identity

One Identity helps organizations get identity and access management (IAM) right. With our unique combination of offerings, including a portfolio of identity governance, access management, privileged management and identity as a service solutions, organizations can achieve their full potential – unimpeded by security, yet safeguarded against threats. Learn more at OneIdentity.com

(c) 2018 One Identity Software International Limited. ALL RIGHTS RESERVED. One Identity, and the One Identity logo are trademarks and registered trademarks of One Identity LLC in the U.S.A. and other countries. For a complete list of One Identity trademarks, please visit our website at www.oneidentity.com/legal. All other trademarks, servicemarks, registered trademarks, and registered servicemarks are the property of their respective owners.

ONE IDENTITY™

syslog-ng.com