ManageEngine
Log360

How Log360 helps Australian organisations with the Notifiable Data Breaches scheme

www.manageengine.com/log-management

Introduction

According to the Notifiable Data Breaches (NDB) scheme, organisations in Australia that fall under the Privacy Act must report eligible data breaches to the Office of the Australian Information Commissioner (OAIC) as well as to the affected individuals. Eligible data breaches are those which compromise an individual's personal data and puts them at risk.

This new regulation is pushing for organisations to re-evaluate their security posture and fill any gaps in their security strategy by implementing proper processes and deploying appropriate tools. This document will offer an overview on how organisations can leverage a security information and event management (SIEM) solution such as **ManageEngine's Log360** to meet the NDB scheme requirements.

What organisations are expected to do

If breached, organisations must first take remedial steps to mitigate the data breach and ensure damage control. In cases where remediation does not mitigate the adverse impact to the affected individuals, then details about the data breach, including the affected individuals, nature of information compromised, possible risk associated with the compromise of personal data, and the recommended response steps must be reported to the OAIC as well as to the affected individuals. Failure to do so will result in non-compliance with the Privacy Act, which, in turn, can lead to severe legal and financial penalties.

Apart from implementing measures to prevent breaches, organisations must ensure they have an audit trail of key security events occurring in their network. This will help them quickly detect, investigate, and mitigate potential breaches at an early stage. Even when a breach can't be mitigated, an audit trail will provide crucial details about the breach when reporting to the OAIC.

Shift the focus to incident detection and response

While preventive measures and security best practices are always important, detection and response mechanisms are essential in combating advanced threats. Security auditing technology plays a major role in this aspect.

Security teams should configure logging in their environment so they can gain more visibility into security events and alerts occurring in their network. Logging not only ensures that security events are being continuously tracked, but also helps security teams identify and analyze events of interest.

Identify critical sources that require auditing

While IT environments vary from business to business, there are some common components found across most enterprises, and auditing them continuously is crucial to ensure security and compliance. These components include:

- Servers
- Domain controllers
- Workstations
- Databases
- Web servers
- Sensitive files and folders
- Routers, switches, firewalls, and IDS and IPS devices
- Endpoint security solutions
- Public cloud infrastructure

Remember: Tracking privileged user access and administrative actions is also an important aspect of SIEM.

Getting started with SIEM

Getting started is easy! First, admins need to identify the log sources and enable auditing for the events that need to be tracked. Next, they should deploy a SIEM solution to leverage the audit trail. This will allow their organisation to periodically review security events with reports; receive alerts for threats; and investigate, respond to, and—if required—report breaches.

Using a proper SIEM solution, security teams can not only thwart breaches at an early stage, but also obtain details when filing a report to the authorities. The powerful security auditing features of Log360, ManageEngine's comprehensive SIEM solution, can do just that.

Key features of Log360

ManageEngine Log360 is a comprehensive security information and event management (SIEM) solution that helps enterprises mitigate external and internal threats with the following capabilities:

- **Log collection:** Collect and analyze log data from all the above mentioned sources to provide actionable information that gives security teams valuable insights into their IT environment.

- **In-depth security auditing**: Generate pre-built audit reports (each of which can be associated to an alert profile) for a wide range of devices and platforms, including Active Directory, firewalls, and databases.

- **Cloud auditing:** Gain visibility into security events occurring on cloud platforms such as Azure, AWS, and Office 365.

- **Alerting:** Alert security teams in real time about events that require their immediate attention, such as account lockouts, security group membership changes, unauthorized access attempts to files or folders, network attacks, and more.

- **Data security:** Discover sensitive data residing in your file servers and implement real-time file integrity monitoring (FIM) to detect attack attempts.

- **Event correlation:** Automatically associate events from different sources to detect suspicious patterns that resemble an attack. Predefined use cases include detecting installation of suspicious software, malicious URL requests, worm activity, and more.

- **Threat intelligence:** Utilize a built-in STIX/TAXII feeds processor and a global IP threat database that can instantly detect known malicious traffic passing through the network as well as outbound connections to malicious domains and callback servers. The advanced threat analytics add-on gives deeper insights into the threats that have been flagged.

- **Incident management:** Automatically raise alerts as tickets to the designated administrator in ServiceDesk Plus or ServiceNow to create an incident resolution process that is swift and accountable.

- **Log forensics and archival:** Backtrack breaches and obtain important forensic information about incidents. The collected logs can be securely archived to revisit when investigating future incidents.

- **UEBA:** Log360's UEBA (user and entity behavior analytics) add-on uses machine learning techniques to detect threats that would have been missed by traditional rule-based detection mechanisms. The add-on detects anomalies in user and system behavior, and assigns risk scores that change dynamically based on the severity of the anomaly. This allows security teams to accurately discover, prioritize, and investigate security incidents.

- **Automated response workflows:** Automate response actions for various security alerts. Workflows for disabling users and computers, killing processes, shutting down systems, and more are built into the solution.

Learn more about Log360.

About the author

Siddharth Sharath Kumar is an IT security and compliance specialist on ManageEngine's product marketing team. He writes articles and e-books, regularly hosts webinars on key IT security topics, and presents at ManageEngine's conferences and other industry events across the globe.