Data on the loose: why it's time to regain control

58 percent of the organisations we analysed had more than 100,000 folders open to all employees and, in total, 21 percent of all the folders in our investigation had no access controls at all.

by Matt Lock, director of sales engineers, UK, Varonis.

Security strategies tend to focus on keeping external threats out of the enterprise network, but many organisations are leaving themselves vulnerable to data breaches with poor internal practices.

In particular, some of the most significant data breaches in recent years have been the result of bad practice around managing and securing data on the network. Varonis recently investigated the extent of this problem by analysing more than six billion files held by 130 organisations as part of its 2018 Global Data Risk Report. With the GDPR introducing strict new requirements on data security, it has never been more important to take control of data.

Open access

The most extensive issue we encountered was a lack of proper control over who could access sensitive data. 58 percent of the organisations we analysed had more than 100,000 folders open to all employees and, in total, 21 percent of all the folders in our investigation had no access controls at all. Worse yet, 41 percent of companies had at least 1,000 sensitive files open to all employees.

Unsecured folders that are open to global access groups – those set to Everyone, Domain Users, or Authenticated Users – are also a major windfall for attackers that have breached the network, granting easy access to key data such as intellectual property and customer data. Poor access control also increases the threat of a malicious insider abusing their position.

Ghosts in the system

Not only are organisations struggling to keep track of what users can access, many also fail to track which accounts exist at all. Many enterprise networks are full of ghost users – accounts which are supposedly inactive but still retain their full capability to login to the network and access files. On average, we found 34 percent of all user accounts in an organisation were actually ghosts. These old accounts are another gift to external attackers, who can use them to move around the network with impunity and are largely unmonitored. Former employees could also log back in after leaving the organisation to access sensitive files – a favoured tactic used by some for gaining goodwill after joining a competing company.

Compounding this issue, 46 percent of organisations also had more than 1,000 users with passwords that never expire. This means that many ghost accounts can be utilised by threat actors months or even years later.

The risk of stale data

Alongside old user accounts, most organisations also have a major problem with old, unused data that is no longer being used in daily operations. We found that on average, 54 percent of all data on the network was stale, and this commonly included sensitive data such as critical information about employees, customers, projects and clients.

Stale data creates an unnecessary storage expense and complicates data management, but also poses a major security risk. The more data on the system, the more damage an intruder or malicious insider can do when they access the network. Additionally, much of this data is subject to regulations such as PCI DSS and the GDPR, exposing the organisation to added liability.

The least privilege approach

One of the best places to start for any organisation seeking to regain control of its data is to sort out file access. Firms need to run a full audit of all servers to identify any data containers such as folders, mailboxes and SharePoint sites, that have global access groups applied to their ACLs (access control lists). These global access groups need to be replaced with tightly managed security groups that ensure only appropriate users have access to sensitive and regulated data. Moving forwards, a least privilege approach should be used for all access permission, with users only accessing as much as they need to perform their roles.

Companies should also work to exorcise their ghost users by ensuring stale accounts are disabled or outright deleted.

Behavioural analysis can be used to understand what constitutes normal user behaviour and better spot inactive users and other behavioural anomalies.

Finally, the way data is collected and stored should follow the principles of privacy by design. This includes minimising the amount of sensitive data that is collected and how long it is stored for and reducing the number of users that can see it, using a least privilege approach. Networks also need to be analysed for stale data and the findings should be either deleted or archived, particularly data that is sensitive or covered by a regulation.

By going back to analyse their current data practices and laying new groundwork to ensure data is collected, stored and accessed securely moving forwards, organisations can gain control of their data and drastically reduce the risk of both internal and external threats.