Lepide

Lepide

Risk Analysis Report

The Lepide Risk Analysis Report is a detailed summary of the potential security threats in your organisation right now. It is based on data collected over 15 days from a sample of your live environment and is designed to highlight security vulnerabilities and recommend remediation.

[The data included in this report is randomly generated as a sample]

DISCLAIMER

The information contained in these documents is confidential, privileged and intended only for the recipient. It may not be published or redistributed without the prior written consent of both Lepide and the recipient.

Lepide

Contents Summary

Permissions & Privileges

Risk Level - Moderate

Knowing who has access to your data and when these permissions change is critical to ensuring you are operating on a policy of least privilege and reducing the risk of privilege abuse.

Risk Summary:

We detected 33 changes to File Server permissions and 29 changes to Exchange Server permissions which may both require further investigation.

High levels of permission changes could indicate data potentially becoming over exposed; which could lead to vulnerabilities and a higher risk of a data breach occurring.

Recommended Actions:

Your organization should be operating on a policy of least privilege where users only have access to the files and folders they need to do their job, nothing more.

We recommend that you regularly review, and create proactive alerts for permission changes.

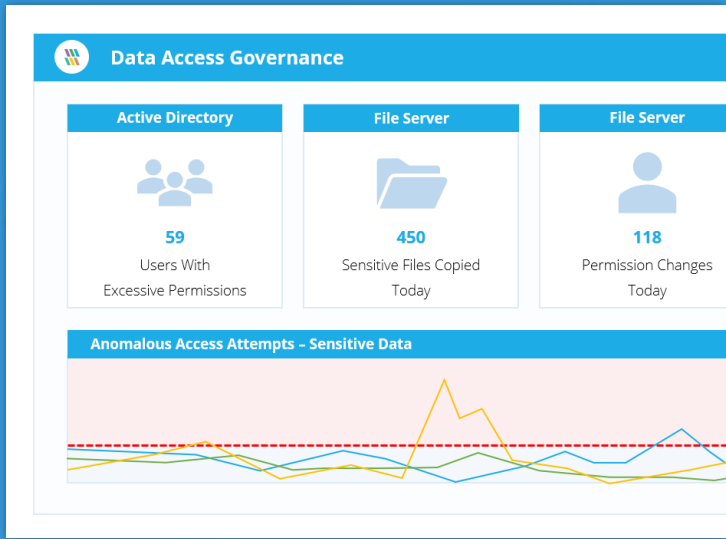
Whenever permission changes occur to your most sensitive data, they need to be analyzed to determine whether they are necessary or should be reversed.

29
Exchange Server Permission Changes

779
Mailbox Modifications

33
File Server Permission Changes

35
AD Group Modifications



User & Entity Behavior

Knowing how your users and entities are interacting with your data is critical to ensuring that data breaches and attacks do not go unnoticed.

Risk Summary:

A high number of failed logons could be indicative of a brute force attack.

Over 10,000 files copied over the analysis period could potentially be an indication of a data breach and drastically increases the threat surface area.

A large number of files being moved and modified could result in data being stored in unsecure locations or being hidden.

Over 24,800 failed filed reads coupled with over 5,000 files renamed could signify a potential ransomware attack in motion, immediate investigation is recommended.

Recommended Actions:

The sheer volume of failed logons, file/folder modifications and file copy events per day makes proactive monitoring essential.

A longer learning period is required to better determine whether these figures are normal for the organization or indicative of ongoing attacks/threats.

A longer learning period will also ensure that our anomaly spotting technology will become more accurate.

Risk Level - High

5,073
Failed Logons

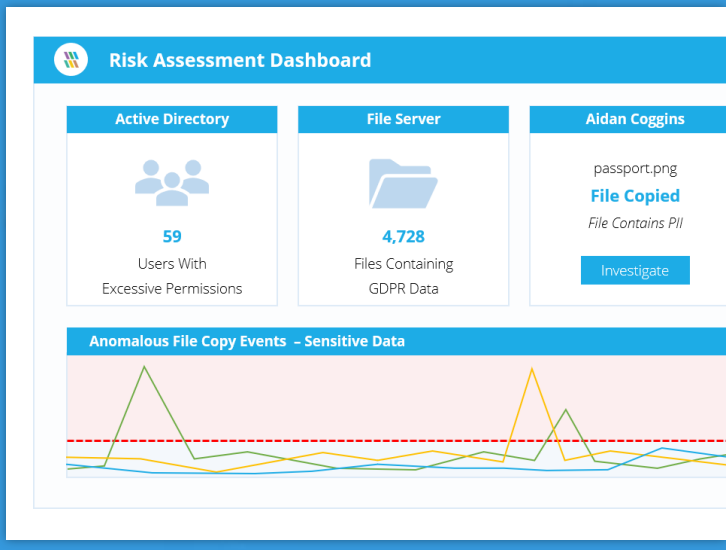
10,535
Files Copied

24,867
Failed File Reads

5,220
Files Renamed

583
Files Moved

38,552
Files Created



States & Changes

Risk Level - High

An important part of data security is understanding whether the infrastructure surrounding the data is secure. If you spot any environment states or changes that pose a risk to data security, action needs to be taken.

Risk Summary:

A large number of inactive /stale users creates a larger attack surface for external threats.

It is recommended that passwords should be rotated on a regular basis to reduce the risk of a user or service account being compromised. It is not recommended to have any accounts where the password is set to never expire.

OU and Sec Group Modifications can potentially lead to unnecessary access being granted to systems and resources that could put your data at risk.

Open shares increase the risk of privilege abuse resulting in data breaches.

Recommended Actions:

Make sure you're operating on a policy of least privilege by reducing the number of open shares to zero. Open shares may leave data vulnerable to exposure.

Create stricter password policies that require all users to change their passwords regularly (every 30 days, for example) and not to share passwords.

Implement adequate security controls and monitor any modifications to your environment to ensure they don't result in over-privileged users.

425
Inactive Users

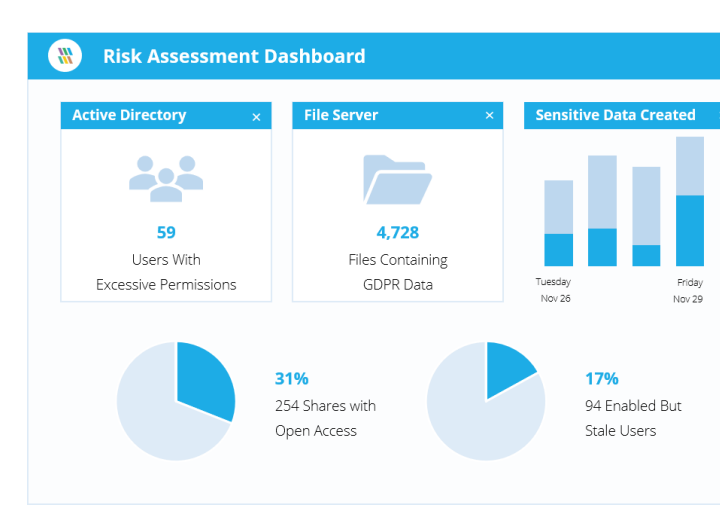
214
Users with Passwords That Never Expire

80
Password Change Attempts

32
OU Modifications

32
Security Group Modifications

3
Open Shares



Risk Summaries

HIGH RISK

18,557,770 Failed Logons
310,551 Files Created
302,083 Files Copied
158,499 Failed File Reads
145,709 Files with Sensitive Information
40,039 Files Renamed
11,036,039 Stale Data
24,508 File Server Permission Changes
16 Active Directory Permission Modifications
3 Exchange Server Permission Changes

Recommendation

You need to determine why you are seeing so many failed logons. Is there a brute force attack underway? Ensure that permission changes are authorized and are not creating users with excessive permissions. Audit file copy events and failed file reads to determine whether sensitive data is at risk.

MEDIUM RISK

1,223 Inactive Users
335 Disabled Users
1,045 Users with Passwords That Never Expire
89,749 OU Modifications
698 Security Group Modifications
940 User Password Change Attempts
3,338 Empty Security Groups
1 Open Shares
248 Mailbox Modifications
66 Users with Administrative Privileges

Recommendation

There is a large attack surface that needs to be addressed. Clean up inactive users, open shares and empty security groups and audit modifications to policies and groups to address this problem. Ensure that none of your users have passwords that are set to never expire. Enable LDAPS.

LOW RISK

0 Admin Policy Template Modifications
0 Security Operations Policy Modifications
0 Event Log Clear Reports
0 Windows Setting Modifications
0 Software Modification Policies
0 Start-up Script Modifications
0 Security Options Policy Modifications
2 Trust Modifications
0 Schema Modifications
0 DNS Zone Modifications
0 Exchange Server Policy Modifications
0 Mailbox Database Modifications

Recommendation

Continuous and proactive scanning of your IT environment is required to ensure that no states or changes pose risk to your data. Continually monitor activity to spot any anomalous user and entity behavior.

Recommendations and Summary

Based on our 15-day analysis of your environment, we have determined the following next steps we believe that you should take to immediately increase your data security.

STEP 1

Reduce your potential attack surface and the chance of privilege abuse by auditing policy and group modifications, implementing stricter password security, removing open shares and cleaning up inactive users and empty security groups.

STEP 2

Upon identifying sensitive data and potential risks and threats that could lead to a security or data breach, ensure there are adequate and efficient security controls in place to effectively mitigate the risk. This could include alerting, monitoring, auditing and a periodic review process which should not be limited to a single team. Encourage effective data owners, department managers and all other personnel responsible for sensitive data to manage these security controls implemented by the DCAP solutions.

STEP 3

Categorize, in order of importance, the highest areas of risk surrounding the silos that require adequate protection starting with the data at most risk first. Also, identify if applicable where there could be a crossover between solution specific functionality based upon storage type but also upon the different security controls required such as DCAP and DLP as an example.

STEP 4

Where applicable, look for native security controls and log sources that can be leveraged and integrated with DCAP specific security solutions. Understand the shortcomings between the different types of security solutions available and through continuously monitoring and reviewing any existing security controls, perform a gap analysis in the existing security strategy and plan for appropriate measure to fill those gaps.

STEP 5

Identify how data is being transferred between data silos and the user interactions surrounding the data. Understand the permissions and privileges being granted to both users and applications/systems and where appropriate, revoke any unnecessary permissions to adopt a least privilege model surrounding the data.

ABOUT LEPIDE

Lepide are the fastest growing provider of data-centric audit and protection solutions to enterprises all over the world. The award-winning Lepide Data Security Platform enables you to put your data at the heart of your security strategy; mitigating the risks of data breaches and helping to meet compliance requirements.

Protecting the Data of Thousands of Organizations Worldwide