Lepide

2020 STATE OF DATA SECURITY REPORT FROM LEPIDE

Over the course of 2019, Lepide conducted over 500 risk assessments with enterprises (over 1000 employees) in 17 different countries across the globe. We have combined the findings of these reports to shed some light on the current state of data security in 2020.

Contents

Your Data Is At Risk

With every passing year, data security becomes more of a priority and concern for enterprises all over the globe. With attacks becoming more frequent, targeted and damaging, it's essential that businesses know where their risks are and how to address them.

Implementing a plan that successfully addresses the risk to your data security can be a complex task. Many IT/Security teams simply do not know where to start.

To help combat this, we have created this report to help identify what the current state of data security is and where you can start to address risk.

Key Statistics

71% Of companies have over **1,600** File Server Modifications made every day.

44% Of companies have over **100,000** failed logons every day.

71% Of companies have over **1,000** inactive users.

31% Of companies have over **1,000** users with passwords that never expire.

91% Of companies have over **1,000** “stale”, sensitive files.

77% Of companies have over **5,000** “stale”, sensitive files.

Permissions & Privileges

71%

Of companies have over **1,600** File Server Modifications made every day.

57%

Of companies have over **6,500** File Server Modifications every day.

29

Mailbox modifications are made on average every day.

2

AD permissions modifications are made on average every day.

3

Exchange Server permissions modifications are made on average every day.

66

The average number of privileged users in an enterprise organization.

Lepide

Permissions & Privileges – What the Stats Mean

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.

High levels of permission changes on any platforms that contain/relate to sensitive data could indicate data potentially becoming over exposed; which could lead to vulnerabilities and a higher risk of a data breach occurring.

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.

User Behavior Analytics

44% Of companies have over **100,000** failed logons every day.

4,086 Files containing sensitive data are copied every day per enterprise.

15,871 Failed file reads every day per enterprise.

2,081 Files renamed every day per enterprise.

1,026 Files moved every day per enterprise.

6,556 Files containing sensitive data created every day per enterprise.

User Behavior Analytics – What the Stats Mean

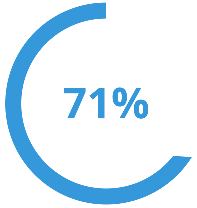
Knowing how your users and entities are interacting with your data is critical to ensuring that data breaches and attacks do not go unnoticed.

A high number of failed logons could be indicative of a brute force attack. High numbers of files copied over could potentially be an indication of a data breach and drastically increases your threat surface area.

A large number of files being moved and modified could result in data being stored in unsecure locations or being hidden. Large numbers of failed filed reads coupled with files renamed could signify a potential ransomware attack in motion, immediate investigation is recommended in this circumstance.

You need to ensure you know where your most sensitive data is located, who has access to it, and what these users are doing with it in order to identify and address risks.

Security States



71%

Of companies have over **1,000** inactive users.

31%

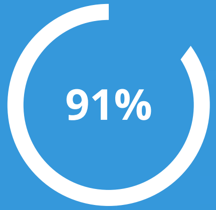
Of companies have over **1,000** users with passwords that never expire.

57%

Of companies have 2 or more open shares.

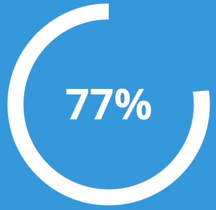
667

The number of OU modifications made every day per enterprise.



91%

Of companies have over **1,000** “stale”, sensitive files.



77%

Of companies have over **5,000** “stale”, sensitive files.

Lepide

Security States – What the Stats Mean

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.

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 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.

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.

Recommendations

STEP 1 – REDUCE YOUR ATTACK SURFACE

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 – GOVERN ACCESS TO SENSITIVE DATA

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 YOUR SECURITY RISKS

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.

Recommendations (Continued)

STEP 4 – LOOK FOR SOLUTIONS TO INTEGRATE

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 – UNDERSTAND YOUR ENVIRONMENT

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.

STEP 6 – TAKE A FREE DATA RISK ANALYSIS

At Lepide, we offer a completely free Data Risk Analysis Report that can help you identify where your biggest areas of risk are. Over the course of a learning period, we use our Data Security Platform to determine where your sensitive data is, who has access to it and what users are doing with it – all as a free service. If you would like to know more about this service, please click here.

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

Western Connecticut Medical Group

HOGE · FENTON

FL FIRSTLEGAL

GE Healthcare

FUJITSU

NHS

Deloitte.

Lepide