Vulnerability Assessment Report

December, 3rd 2023

System Description

The environment consists of a Domain Controller running Active Directory with 1000 users and a fleet of workstations that all of them can sign into. Connecting more servers would be no problem in the future. No backup of the main server exists.

Scope

The scope of this assessment is today only.NIST SP 800-115 is used to guide the analysis of the workstation.

Purpose

- How are the computers valuable to the org? **They are instrumental in the process of dealing with customers.No work could be completed without them.**
- Why is it important to secure the workstations? **A data leak from the server employees connect to can cause irreversible damage and tarnish the reputation of the company.**

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Disgruntled employee	Delete critical files	1	3	3
Phishing attack	Takeover an account	2	3	6
Out of date software/ Misconfiguration	Exploit vulnerabilities	2	3	6

Approach and Remediation Strategy

Conduct security training for all employees on the risk of phishing.Rollout 2fa and enforce a strict password policy. Practice principle of least privilege. Make sure the IT department rolls out the most up to date software whenever possible and keep a close eye on the network.