Mini-Project 26: Security Assessment

Executive Summary

The computing environment in this scenario is particularly vulnerable and would not
It is vital to the security posture of the company neglect the vulnerabilities no longer
afer and more secure environment.

Number	Observation	Risk
1	Too much admin access to Windows and Unix.	Excessive access of any capacity is a massive root cause of many different attacks. It is also considered not satisfactory to some security frameworks. When people have access to higher levels of access and privileges they are essentially able to cause more damage and be able to negate and bypass certain security measures. Another aspect of having too much privilege is that people are human and humans make mistakes. For example by having too much power a user could accidentally press a button that otherwise they wouldn't have had available if the permissions were correctly assigned.
2	Password configurations may not be set properly	Basically all three aspects of the CIA triad are susceptible to be breached under this threat of having misconfigured password complexity. Once an attacker has access especially at the admin or root level catastrophic events can follow. Access and authorization are two of the most important aspects of security.
3	Back up tapes are suspect	when assets are suspect it is probable to suggest breach of integrity of the files.

Mini-Project 26: Security Assessment

Executive Summary

The computing environment in this scenario is particularly vulnerable and would not
It is vital to the security posture of the company neglect the vulnerabilities no longer
afer and more secure environment.

Number	Observation	Risk
4	Unauthorized code changes could be occuring	Unauthorized code changes pose significant risks to software integrity, security, and availability. These changes can introduce vulnerabilities, such as backdoors or malicious code injections, compromising the confidentiality, integrity, and availability of data and systems. Additionally, unauthorized modifications may lead to functionality issues or system instability, causing service disruptions or downtime.
5	Alternate power source may not be reliable if main power fails	When a risk to availability as strong as this is presented it is one that must be correected as soon as possible not only because it could shut off the assets but because it could actually damage them as well.
6	Improper database access could be taking	The risks that are aligned with this risk are quite extensive and highly dangerous to an organizations database. This is a massive breach to integrity and confidentiality if any of the database contents falls into the hands of an attacker.
7	Policies and procedures are outdated	Outdated policies and procedures can lead to influidity of business as well as security endeavors ofr an organization. It is also important to keep in mind certain policies and proccedures are required by some frameworks to be considered compliant. It is all in all a great practice to always try to be upto date and keep an open mind to maintain a fluid but efficient and defined structure of policies.

Mini-Project 26: Security Assessment

Executive Summary

The computing environment in this scenario is particularly vulnerable and would not
It is vital to the security posture of the company neglect the vulnerabilities no longer
afer and more secure environment.

Number	Observation	Risk
8	Remote access is performed via RDP from Internet	Remote access is one of the most dangerous forms of access just because the attacks are almost limitless with this form of access. It is essentially the same as sitting directly in front of the computer itself. If an attacker was to successfully gain access to this it is just about the worst that could happen on every aspect of the CIA triad. It could give attackers access to data, and system configurations which could also lead to data exfiltration.

Assessed by: Xavier Nieves

be compliant with security frameworks. and correct them in order to maintain a

Severity	Recommendation
In terms of severity, the levels as scored by the CVSS would score quite high because of the fact that actions taken at the root or admin level could be a lot more damaging than a user with lesser privileges. It is also important to understand that the root and admin level of permissions are simply something to stay away from unless absolutely necessary for some actions that are required. Another key aspect of the threat level is what exactly is on the local host that could be more damging than others such as top secret documents and files or projects as well.	When it comes to too much access at the admin level the easiest format to fix this is by applying the concept of least privilege only giving employees access to what they need for their daily duties and or specialized priviliges for those that need it. It is also important to keep in mind the fact that by doing so they are reducing the attack surface as well as the "mistake surface" as hunmans are humans and when having too much power they could accidentally perform an action that otherwise wouldn't have been possible. It is also important to audit these permissions at least on a quarterly basis to ensure you are compliant with relevant security frameworks.
The severity of the risk according to the CVSS would grade substantially high just because of the access to essentially a users privileges co uld be quite damaging and neglects the confidentiality portion of the CIA triad. It is important to know that any form of a vulnerability that grants access is one of the most dangerous. Access is what a high level threat would want and leaving a vulnerability that is often exploited is not good for the overall security posture of an organization.	Password configurations are quite simple to setup and easy to make robust. This can be done by ensuring the complexity of the passwords is set to a minimum that is compliant with relevant security frameworks and 2FA can also be made available for better security. This can be applied a multitude of ways such as a smart card or a physical token.
The severity would be quite high according to the CVSS simply because of the fact that it directly harms the cohesion of the CIA triad therefore harming the security posture of the organization.	When any form of data is suspect it is important to investigate them and ensure they are or aren't. Aftwerwards, the real work can begin by either deleting and restoring from previously untampered tapes or by ensuring all of the future ones are unable to be tampered with by setting the correct access controls and also auditing them for any alterations.

Assessed by: Xavier Nieves	
be compliant with security frameworks. and correct them in order to maintain a	

Severity	Recommendation
After Assessing how unauthorized code changes would be scored using the CVSS it would have a higher score simply because of the effects that it would have on the integrity and security of the effected software.	The most important changes that are efficient relevant to this risk is implementing some form of IDS and access controls to be able to know who and when these events are happening. Also applying some form of two step editing which requires authorization from those at admin levels in order for the changes to go through. Overall, the main task in ensuring the security of the code is being able to identify when anomylous code changing is happening to be able to combat it and use each case as a lesson to further secure your coding environment.
This is one of the most overlooked forms of vulnerability but also one of the most compromising simply because it directly relates to availibility and it could even be a potential hazard not only to the hardware but software as well.	To diminish the rate in which these events could happen it is important to instill some form of testing to ensure that in the case of an emergency situation and the loss of power to the main grid occurs that the backups are just as efficient and last long enough in order to repair the mainframe of power.
Improper database access controls are absolutely vital to the health and security posture of a database and improper controls leads to severe consenquences affecting the CIA triad of the organization.	Database security being one of the most important it requires some of the robust access controls and continuous monitoring for improper permissions and privileges incorrectness. It would also be important to link the login data to a SIEM in order to easier monitor activity within the database.
Out of date policies and procedures are often at the heart of morale loss within staff and leadership and can also harm the reputation of an organization. It is something that can also lead to loss of customers if the corresponding policies effect them as well as business partners and stakeholders. This risk is substantially severe because of the diverse effects it can unleash.	When it comes to policies it is almost never a single person creating and enforcing them. Therefore it should be a team effort between mangement and leaders as wellas stakeholders to get different perspectives as well as get the best interests of all corners of the organization. It is also important to keep up with current best practices specifically even more so those pertaining to security and workplace behavior.

Assessed by: Xavier Nieves	
t be compliant with security frameworks. · and correct them in order to maintain a	
Severity	**Recommendation**
The severity of this particular risk is quite high because of the fact that any risk that pertains to access specifically remote access are some of the most devastating as it can result in tampering of data, exfiltration as well as loss of confidentiality. Remote access and access controls in general are one of the first layers of defense for a company and must be one of the most robust.	To mitigate the risks with this specific it would be important to put in place very stronmg access controls and limit the access in any other way possible such as only giving the capability to certain computers by tying them to their IP and whitelisting them. It is thin ice to walk on working with remote access and it is impoortant that the ones that can access it are only those who have authorization.