Step 4: Risk Treatment

Step 4.1: Risk Treatment and Calculation of Residual Risk for Supporting Assets

Supporting Assets (same as specified in step 2.1)	Threats (same as specified in step 3.1)	Vulnerability (same as specified in step 3.1)	Pre- Controls	Post-Controls	Reviewed Impact (from step 3.1)	Likelihood (from step 3.2)	Residual Impact	Residual Likelihood	Residual Risk level (from Table 3.1)
Third Party Authentication Server Appliances	Password attacks on user credentials	Week password	Enforce strong password assignement	Block accounts	4	4	3	2	LOW
			Password hashing + salting	Notify users and enforce password reset					
	MITM attacks	Faulty server authentication configuration	Enforce the use of the latest TLS version	Block accounts	4	4	3	2	LOW
			DIsable support for older TLS versions	Notify users and enforce password reset					
	DDoS attacks	No load balancing and/or DDoS protection service	Adopt DDoS protection service	Deep inspect traffic and blacklist non-legitimate users	4	3	3	2	LOW
	Equipment tampering	Broken physical access control	Adopt CCTV cameras	Backup the machine for forensics	4	3	2	2	LOW
			Backup server configuration	Reset server and restore configuration					
			Use biometrical access control						
Third Party Authentication Database Appliances	SQL injections	No input sanitization	Install firewall to block ports TCP 1433, 4022, 135, 1434, UDP 1434	If tables are exfiltrated, block accounts	4	4	1	2	LOW
			Periodically backup users data	If tables are exfiltrated, notify users and enforce password reset					
			Update software to adopt input sanitisation	If tables are dropped, restore data using bakup					
	Password attacks on admin credentials	Poor credential managing	Enforce strong password assignement	Block admin account	4	4	3	3	MEDIUM
			Backup database configuration	Notify admin and enforce password reset					
			Password hashing + salting	If needed restore database configuration and users data					
	Data leak	Poor permission management	Setup transaction audit for the database	Block accounts	3	2	2	2	LOW
			Adopt least priviledge access control	Notify users and enforce password reset					
Generic 2FA Server Appliance	Password attacks on user credentials	Week password	Enforce strong password assignement	Block accounts	4	4	3	2	LOW
			Password hashing + salting	Notify users and enforce password reset					
	MITM attacks	Faulty server authentication configuration	Enforce the use of the latest TLS version	Block accounts	3	4	3	2	LOW
			DIsable support for older TLS versions	Notify users and enforce password reset					
	DDoS attacks	No load balancing and/or DDoS protection service	Adopt DDoS protection service	Deep inspect traffic and blacklist non-legitimate users	4	3	3	2	LOW
Generic 2FA Database Appliance	SQL injections	No input sanitization	Install firewall to block ports TCP 1433, 4022, 135, 1434, UDP 1434	If tables are exfiltrated, block accounts	4	4	1	2	LOW
			Periodically backup users data	If tables are exfiltrated, notify users and enforce password reset					
			Update software to adopt input sanitisation	If tables are dropped, restore data using bakup					
	Password attacks on admin credentials	Poor credential managing	Enforce strong password assignenment	Block admin account	4	4	3	3	MEDIUM
			Backup database configuration	Notify admin and enforce password reset					
			Password hashing + salting	If needed restore database configuration and users data					
	Data leak	Poor permission management	Setup transaction audit for the database	Block accounts	3	3	2	2	LOW
			Adopt least priviledge access control	Notify users and enforce password reset					
Input Officials	(spear) Phishing attacks	Untrained users	Adopt anti-spam software for mail agent and / or SMTP server	Enforce credential reset	4	4	3	3	MEDIUM
			Train users	Check audit for misconduct					
	Disease	Officials can get ill	Select and train backup officials	Switch to backup official	4	3	1	3	LOW
	Blackmailing	Poor personal data confidentiality	Run background checks on the official to select	Disaster recovery	4	3	4	2	MEDIUM
				Check logs for misconduct					
CSB / GSB personeel	(spear) Phishing attacks	Untrained users	Adopt anti-spam software for mail agent and / or SMTP server	Enforce credential reset	3	4	3	3	MEDIUM
			Train users	Check audit for misconduct					
	Disease	Officials can get ill	Setup a VPN for remote access	Enable credential for user and let him/she access from home	3	2	1	3	LOW
	Blackmailing	Untrained users	Run background checks on the official to select	Disaster recovery	3	3	3	2	LOW
				Check audit for misconduct					