Step 3: Risk Evaluation

Step 3.2: Risk Evaluation

Supporting Assets(same as specified in step 2.1)	***Threats (same as specified in step 2.1)***	***Vulnerability (same as specified in step 2.1)***	***Reviewed Impact (from step 2.1)***	***Likelihood (from step 2.2)***	***Risk level (from Table 3.1)***
Third Party Authentication Server Appliances	*Password attacks on user credentials*	*Week password*	4	4	HIGH
	MITM attacks	*Faulty server authentication configuration*	4	4	HIGH
	DDoS attacks	*No load balancing and/or DDoS protection service*	4	3	HIGH
	Equipment tampering	*Broken physical access control*	4	3	HIGH
Third Party Authentication Database Appliances	*SQL injections*	*No input sanitization*	4	4	HIGH
	Password attacks on admin credentials	*Poor credential managing*	4	4	HIGH
	Data leak	*Poor permission management*	3	2	LOW
Generic 2FA Server Appliance	*Password attacks on user credentials*	*Week password*	4	4	HIGH
	MITM attacks	*Faulty server authentication configuration*	3	4	HIGH
	DDoS attacks	*No load balancing and/or DDoS protection service*	4	3	HIGH
Generic 2FA Database Appliance	*SQL injections*	*No input sanitization*	4	4	HIGH
	Password attacks on admin credentials	*Poor credential managing*	4	4	HIGH
	Data leak	*Poor permission management*	3	3	MEDIUM
Input Officials	*(spear) Phishing attacks*	*Untrained users*	4	4	HIGH
	Disease	Officials can get ill	4	3	HIGH
	Blackmailing	Poor personal data confidentiality	4	3	HIGH
CSB / GSB personeel	*(spear) Phishing attacks*	*Untrained users*	3	4	HIGH
	Disease	Officials can get ill	3	2	LOW
	Blackmailing	*Untrained users*	3	3	MEDIUM
Diginetwerk	*Coremelt*	*Communication links have limited bit-rate*	4	2	MEDIUM
	Unauthorized wired connection	*Broken physical access control to routers*	5	3	HIGH
	Router crash	*Poor load balancing*	4	3	HIGH
	Broken link	*Poor network redundancy*	4	3	HIGH
	Downtimes	*Hardware needs power*	4	2	MEDIUM
	Routing loop	*Poor router and L3 switch configuration testing*	4	3	HIGH
VPN	Unauthorized access to virtual network	Poor third party policies	3	4	HIGH
Firewall Appliance	*System crash*	*Poor load balancing*	4	3	HIGH
	Configuration file tampering	*Broken authentication*	4	4	HIGH
Virtual Desktop Infrastructure (Citrix)	Hyperjacking	Broken authorization&authentication	5	4	HIGH
	Ransomware	Poor controls on installed software	4	4	HIGH
	Hypervisor server crash	Faulty load balance on Citrix delivery controllers	4	3	HIGH
DHV Software	Software crash	Unhadled software exeptions	4	2	MEDIUM
	False Data Input	Faulty access control	4	3	HIGH
Citrix server room(s)	Floods	Lack of flood preventing infrastrucutre	4	3	HIGH
	Fires	Faulty fire coutermeasures	4	2	MEDIUM
	Theft of equipment	Poor physical access control	4	4	HIGH
	Overheating	Faulty cooling system	4	3	HIGH
GSB PCs	Damaged hardware	Poor manifacturing	4	3	HIGH
	Physical key loggers	Poor physical access control	3	4	HIGH
Secure Store for GSB PCs	Flood	Lack of flood preventing infrastrucutre	4	3	HIGH
	Fires	Faulty fire coutermeasures	4	2	MEDIUM
	Theft	Poor physical access control	4	4	HIGH
	Hardware damaging	Poor physical access control	4	4	HIGH
GSB LAN gateway	Network tapping	Broken physical acces control	2	4	MEDIUM
	Configuration tampering	Broken access control	3	4	HIGH