Step 2: Threat Evaluation

Step 2.1: Vulnerabilities & Threat Scenarios Evaluation

Supporting Asset	***Threat***	***Vulnerability***	***Primary Assets***																																		***Inherited impact***	***Reviewed Impact***
			Input officials' credentials			***GSB / CSB users' credentials***			***Ballots data input***			**Third Party authentication service**			**2 Factor Authentication service**			**Software Distribution (Virtual Desktop**			**Result computation**			**Web Application Firewall**			**Diginetwerk routing / communication**			**GSB LAN to Citrix communication**			**Inport check, approval and signing**				
			C	I	A	C	I	A	C	I	A	C	I	A	C	I	A	C	I	A	C	I	A	C	I	A	C	I	A	C	I	A	C	I	A	MAX	<=
			3	4	4	3	4	4	3	4	4	2	3	3	2	4	4	1	5	4	1	5	4	2	4	3	3	5	4	2	3	3	1	3	3		
Third Party Authentication Server Appliances	Password attacks on user credentials	Week password				3	4	4				2																					1			4	4
	MITM attacks	Faulty server authentication configuration				3	4	4				2																					1			4	4
	DDoS attacks	No load balancing and/or DDoS protection service						4						3																					3	4	4
	Equipment tampering	Broken physical access control				3	4	4				2	3	3																					3	4	4
Third Party Authentication Database Appliances	SQL injections	No input sanitization				3	4	4						3																						4	4
	Password attacks on admin credentials	Poor credential managing				3	4	4				2	3	3																						4	4
	Data leak	Poor permission management				3						2																								3	3
Generic 2FA Server Appliance	Password attacks on user credentials	Week password	3	4	4	3	4	4							2	4	4																			4	4
	MITM attacks	Faulty server authentication configuration	3			3									2																					3	3
	DDoS attacks	No load balancing and/or DDoS protection service			4			4									4																			4	4
Generic 2FA Database Appliance	SQL injections	No input sanitization	3	4	4	3	4	4	3	4	4						4																			4	4
	Password attacks on admin credentials	Poor credential managing	3	4	4	3	4	4	3	4	4				2	4	4																			4	4
	Data leak	Poor permission management	3			3																														3	3
Input Officials	(spear) Phishing attacks	Untrained users	2	3					3	4																										4	4
	Disease	Officials can get ill								4	4																									4	4
	Blackmailing	Poor personal data confidentiality	2	3					3	4	4																									4	4
CSB / GSB personeel	(spear) Phishing attacks	Untrained users				2	3																													3	3
	Disease	Officials can get ill																																	3	3	3
	Blackmailing	Untrained users				2	3																										1	3	3	3	3
Diginetwerk routing	Coremelt	Communication links have limited bit-rate									4			3			4			4									4			3				4	4
	Unauthorized wired connection	Broken physical access control to routers																									3	5	4	2	3	3				5	5
	Router crash	Poor load balancing									4			3			4			4									4			3				4	4
	Broken link	Poor network redundancy									4			3			4			4									4			3				4	4
	Downtimes	Hardware needs power																											4			3				4	4
	Routing loop	Poor router and L3 switch configuration testing																											4			3				4	4
VPN	Unauthorized access to virtual network	Poor third party policies				3						2																					1			3	3
Firewall Appliance	System crash	Poor load balancing									4									4						3									3	4	4
	Configuration file tampering	Broken authentication									4									4				2	4	3									3	4	4
Virtual Desktop Infrastructure (Citrix)	Hyperjacking	Broken authorization&authentication	3						3	4	4							1	5	4	1	5	4										1	3	3	5	5
	Ransomware	Poor controls on installed software									4									4			4												3	4	4
	Hypervisor server crash	Faulty load balance on Citrix delivery controllers									4									4			4												3	4	4
DHV Software	Sotware crash	Unhadled software exeptions									4												4													4	4
	False Data Input	Faulty access control								4																										4	4
Citrix server room(s)	Floods	Lack of flood preventing infrastrucutre			4															4			4			3									3	4	4
	Fires	Faulty fire coutermeasures			4															4			4			3									3	4	4
	Theft of equipment	Poor physical access control	3		4													1		4	1		4	2		3							1		3	4	4
	Overheating	Faulty cooling system			4															4			4			3									3	4	4
GSB PCs	Damaged hardware	Poor manifacturing									4																									4	4
	Physical key loggers	Poor physical access control	3			3			3																											3	3
Secure Store for GSB PCs	Flood	Lack of flood preventing infrastrucutre									4																									4	4
	Fires	Faulty fire coutermeasures									4																									4	4
	Theft	Poor physical access control									4																									4	4
	Hardware damaging	Poor physical access control									4																									4	4
GSB LAN gateway	Network tapping	Broken physical acces control																									2			2						3	2
	Configuration tampering	Broken access control																									2	3	3	2	3	3				3	3