Step 2: Threat Evaluation

2.2 Likelihood Assessment on Supporting Assets

Supporting Asset	Threat	Vulnerability	Likelihood Areas								
			Skills	Means	Opportunity	Profit	Attention	Impunity	Detection	Overall Likelihood (2.2)	Justification
Third Party Authentication Server Appliances	Password attacks on user credentials	Week password	3	4	5	1	4	4	3	4	Password attacks are really common, especially in systems that have strong
	MITM attacks	Faulty server authentication configuration	4	4	3	1	4	4	4	4	MITM attacks do not require paticular means or skills. This entail an high
	DDoS attacks	No load balancing and/or DDoS protection service	2	2	5	1	5	4	2	3	DDoS attacks require a grat numbers of slaves that need to be bought or
	Equipment tampering	Broken physical access control	3	3	5	1	5	2	2	3	High chance of punishment and detection
Third Party Authentication Database Appliances	SQL injections	No input sanitization	4	4	5	1	5	4	3	4	Common attack, low skills needed, low chance of punishment and detection if
	Password attacks on admin credentials	Poor credential managing	3	4	5	1	5	4	4	4	Password attacks are really common, especially in systems that have strong
	Data leak	Poor permission management	1	1	2	1	5	2	2	2	Need lot of skills and means to convince someone to leak information.
Generic 2FA Server Appliance	Password attacks on user credentials	Week password	3	4	5	1	4	4	3	4	Also here, despite of identity control, Password attacks are really common,
	MITM attacks	Faulty server authentication configuration	4	4	3	1	4	4	4	4	MITM attacks do not require paticular means or skills. This entail an high
	DDoS attacks	No load balancing and/or DDoS protection service	2	2	5	1	5	4	2	3	DDoS attacks require a grat numbers of slaves that need to be bought or
Generic 2FA Database Appliance	SQL injections	No input sanitization	4	4	5	1	5	4	3	4	Common attack, low skills needed, low chance of punishment and detection if
	Password attacks on admin credentials	Poor credential managing	3	4	5	1	5	4	4	4	Password attacks are really common, especially in systems that have strong
	Data leak	Poor permission management	5	2	2	1	5	2	3	3	Need lot of skills and means to convince someone to leak information.
Input Officials	(spear) Phishing attacks	Untrained users	3	4	5	1	4	3	4	4	Also here, despite, but it's the information needed to run a phishing
	Disease	Officials can get ill								3	There are great number of official, there is a reasonable possibility that
	Blackmailing	Poor personal data confidentiality	3	2	5	1	4	3	3	3	Less probable of phishing, since it's usually harder to obtain information to
CSB / GSB personeel	(spear) Phishing attacks	Untrained users	3	5	5	1	4	3	4	4	Also here, despite, but it's the information needed to run a phishing
	Disease	Officials can get ill								2	There are small number of chairmen and employee compared to the input
	Blackmailing	Untrained users	3	2	5	1	4	3	3	3	Less probable of phishing, since it's usually harder to obtain information to
Diginetwerk	Coremelt	Communication links have limited bit-rate	1	2	5	1	5	4	1	2	Need access to private network, great skills needed
	Unauthorized wired connection	Broken physical access control to routers	4	3	5	1	5	2	2	3	Physically accessing a routers room yelds an high chance of detection and
	Router crash	Poor load balancing								3	If the network is badly designed, a router crash is fairly possible
	Broken link	Poor network redundancy								2	SImilar as above
	Downtimes	Hardware needs power								2	It is remotely possible that during the operational time of our system that a
	Routing loop	Poor router and L3 switch configuration testing								3	If the level 3 network services has not been correctly set up, routing loops are
VPN	Unauthorized access to virtual network	Poor third party policies	2	3	5	1	5	4	4	4	Breaking VPN access control requires high skills, but once access has been
Firewall appliance	System crash	Poor load balancing								3	If the firewall wasn't chosen and configured carefully, it's fairly possible
	Configuration file tampering	Broken authentication	4	3	5	1	4	3	3	4	If the authentication is broken, the most difficult part is to find the vulnerability
Virtual Desktop Infrastructure (Citrix)	Hyperjacking	Broken authorization&authentication	3	3	5	1	5	4	2	4	Similar as for configuration tampering in firewall
	Ransomware	Poor controls on installed software	3	3	5	5	5	3	2	4	High likelihood since it can produce an high profit
	Hypervisor server crash	Faulty load balance on Citrix delivery controllers								3	If the virtualization server isn't properly configured, there it is possible for it to
DHV Software	Sotware crash	Unhadled software exeptions								2	If there are unhadled software exeptions, it is possible for the software
	False Data Input	Faulty access control	3	2	3	1	5	4	3	3	Low chance of punishment, but also high skills needed to breach a private
Citrix server room(s)	Floods	Lack of flood preventing infrastrucutre								3	Flood are not rare in the Netherlands
	Fires	Faulty fire coutermeasures								2	Fire outbrackes are not a common thingh in server rooms
	Theft of equipment	Poor physical access control	5	5	5	3	4	2	1	4	If there is a poor access control, it is likely that someone will steal something
	Overheating	Faulty cooling system								3	It is probable that with a faulty cooling system temperature will rises to cause
GSB PCs	Damaged hardware	Poor manifacturing								3	There are a lot of GSB PCs, it can happen that a PC is damaged
	Physical key loggers	Poor physical access control	4	4	5	1	5	2	2	4	Similar to hardware damaging, main difference is that some skills and means
Secure Store for GSB PCs	Flood	Lack of flood preventing infrastrucutre								3	Flood are not rare in the Netherlands
	Fires	Faulty fire coutermeasures								2	Fire outbrackes are not a common thingh
	Theft	Poor physical access control	5	5	5	3	4	2	1	4	If there is a poor access control, it is likely that someone will steal something
	Hardware damaging	Poor physical access control	5	5	5	1	4	2	1	4	Requires no skill, especially if there is no access control. HIgh chance of
GSB LAN gateway	Network tapping	Broken physical acces control	4	4	5	1	4	2	2	4	Similar to key loggers for GSB PCs
	Configuration tampering	Broken access control	3	5	5	1	4	3	3	4	Similar to network tapping, requires higher skills, but can be done remotely,