University of Trento

Department of Information Engineering and Computer Science

The Votes Counting Software Case Study

Security and Safety Engineering Qualitative Assessment Report

Riccardo Gennaro

June 15, 2023

Contents

Executive Summary

This work aims at assessing the security posture of the new Dutch centralized system for vote counting. In this report, the core services, information, and processes are analyzed. Also, the impacts and likelihoods of the possible incidents tied to these processes are estimated. A great number of high-rating threats have been found.

Furthermore, an acceptable level of risk is defined to produce a set of security controls to apply before and after an incident.

After the application of these security measures, no severe-rating threats have remained.

Work submitted in partial fulfillment for the course of Security and Safety Engineering – Vrije Universiteit Amsterdam - a.a. 2022/2023

This work is original, has been done by the undersigned student, and has not been copied or otherwise derived from the work of others not explicitly cited and quoted. The undersigned student is aware that plagiarism is an offense that may lead to failure of the course and more severe sanctions.

Target of evaluation

This work aims at producing an assessment of the procedures that interest the process of uploading and aggregating the Dutch election results. More specifically, we want to analyze the processes of inputting the election results of the commonalities, uploading such results to a centralized server, and computing and approving the aggregated result of the election.

To do so, some assumption had to be made. As can be seen in figure 1 the following was assumed:

- the authentication process is split in a first-party 2FA service, and in a third-party MFA service, depending on the user role.
- the third-party MFA service has access to the private WAN via VPN tunneling.
- The used VPN is a third-party service.
- The private WAN is relying on a third-party ISP infrastructure.

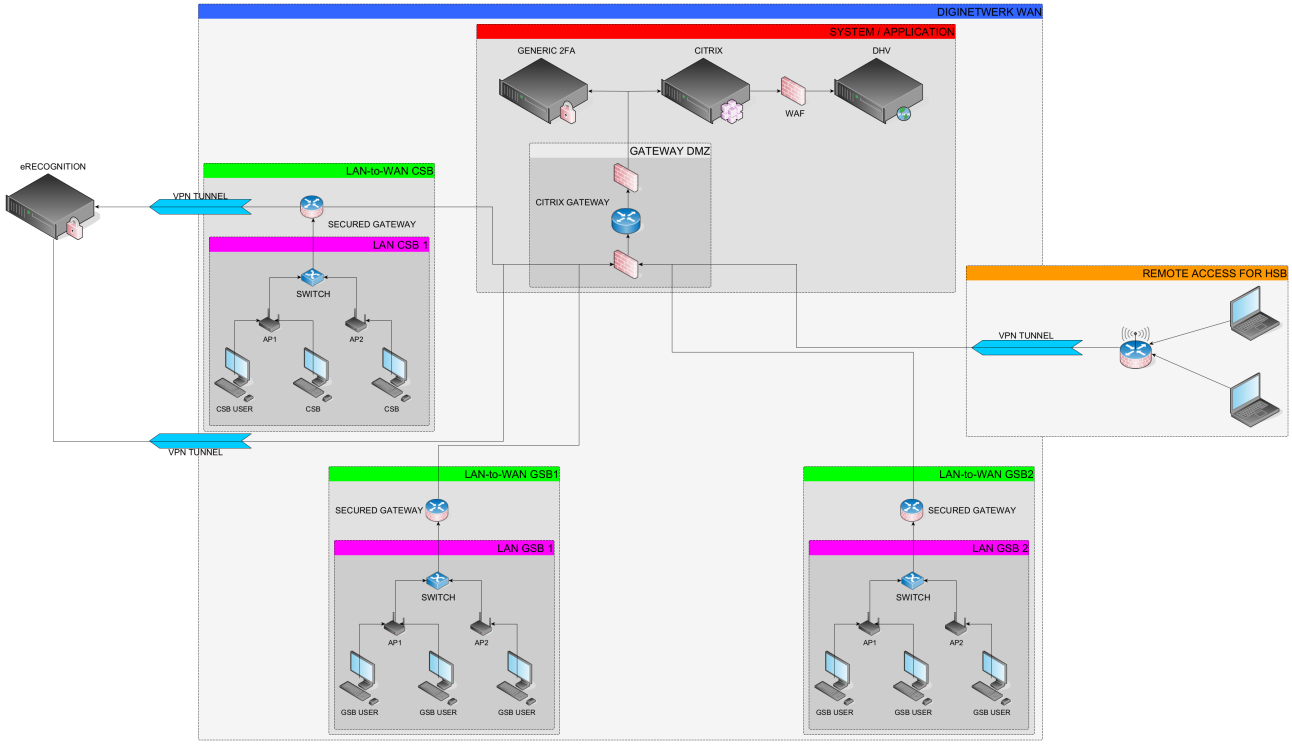

Figure 1: High-level assumed network topology

Summary of findings

During the study of the scenario conducted following the SecRAM2.0 methodology[3], a satisfying number of assets were analyzed. In particular, it became apparent that multiple physical and technical vulnerabilities were left untreated. More specifically, there was a lack of documentation regarding the `Diginetwerk` private network, the `Citrix` virtualization infrastructure, and both the first-party and third-party authentication services.

For all of these assets, sets of threats and vulnerabilities were provided. These sets included infrastructural, software, and configuration vulnerabilities. Regarding `Diginetwerk`, we found that it was exposed to availability attacks like DDoS and Coremelt, but also there were no mechanisms in place to prevent router crashes, downtimes, and other technical issues.

For `Citrix`, the risk of hyperjacking, ransomware, and server crashes was discussed; while for the authentication services, the eventuality of password attacks, equipment tampering, and data leaks was taken into consideration. Also, natural disasters and purposeful damages to the equipment were analyzed.

To reduce the impact and likelihood of a given incident a number of pre and post-incident controls have been proposed. Since this infrastructure is used for a time limited to the one of the elections, we tried to propose a set of moderately costly solutions, avoiding the adoption of full-scale disaster recovery sites. These proposals range from configuration testing to the adoption of physical security and DDoS prevention services.

Update: out of the reported CVEs, four were chosen to be mitigated

- `CVE-2016-7406`
- `CVE-2018-6683`
- `CVE-2021-22927`
- `CVE-2022-38652`

The listed vulnerabilities have `high` or `critical` base score. Also, all of the above greatly impact on the integrity of the data, a property crucial for an election. For these reasons, this CVEs were deemed in urgent need of mitigation.

Risk Analysis

Impact assessment

During this first step, eleven primary assets were identified. Among these assets, three were dimmed essential

- `Software distribution`: the software distribution service is used to distribute the software agent needed to communicate with the virtualization service. Without it, municipalities cannot access the centralized software.
- `Diginetwerk routing&communication`: similarly to the software distribution service, also without a function WAN municipalities cannot access the virtualization server and the authentication services.
- `Result computation`: the result computation is carried out by the DHV software and is essential to output a valid election result.

We didn't take into consideration the endpoint protection service and the third-party security operation center since we deemed those of secondary importance.

1.1. Primary Asset (PA) Identification				
Primary Asset ID	***Primary Asset Name***	***Type (information/service)***	***IT Domain(s)***	***Justification***
PA1	*Input officials' credentials*	information	System / Application	The credential that the two input officials use to log in with the 2FA service in order to enter the ballot counting results
PA2	*GSB / CSB users' credentials*	information	System / Application	The credential that the municipalities members use to log in with the 2FA service in order to check the ballot counting results
PA3	*Ballots data input*	service	User / Workstation	Operation consisting in the insertion of the results in the addition software
PA4	Third Party authentication service	service	Remote Access	Authentication service used by CSB / GSB chairmen
PA5	2 Factor Authentication service	service	System / Application	Generic 2FA authentication service used by input officials and GSB members
PA6	Software Distribution (Virtual Desktop Client)	service	WAN	The software can be retrieved via the digital network. The sotware is available centrally
PA7	Result computation	service	System / Application	The DHV software computes the seats' distribution based on the polling results
PA8	Web Application Firewall	service	System / Application	Firewall deployed between the Virtual Desktop Environment and the DHV application (business logic) that filters and monitors HTTP traffic
PA9	Diginetwerk routing / communication	service	WAN	Packets routing is an essential service offered by the private WAN.
PA10	GSB LAN to Citrix communication	service	LAN	For uploading the resaults, the GSB workstations must be able to contact the Citrix service
PA11	Import check, approval and signing	service	Remote Access	It is required that the GSB/CSB users check and sign the results

Figure 2: Table of primary assets

Following this step, the impacts of potential incidents regarding the CIA triad were estimated.

Supporting Asset Identification & Valuation

In figure 3 the impact assessment is reported.

As we can see from the assessment, the potential compromises with higher overall impact are the ones tied to the integrity of the services of `Software distribution`, `Diginetwerk routing&communication`, and `Result computation`. Also, we can observe that the impact on personnel, the economy, and the environment is estimated to be 1.

Instead of just using the maximum of impacts, the overall impact is computed by applying a weighted average of capacity, performance, branding, and regulatory. Since the branding impact is almost always high (except for third-party incidents) because the election is an event of national matter, and because we believe that capacity and performance has higher priority, we put higher weight 1 on the latter, and 0.5 on the first two indexes.

In figure 4 the linkage between the primary and supporting assets can be observed. For example, we found that the process of inputting the ballots data has the following supporting assets

- `Input Officials`
- `Diginetwerk`
- `Virtual Desktop Infrastructure (Citrix)`
- `DHV Software`
- `GSB PCs`
- `Secure Store for GSB PCs`

1.2 Impact Assessment on Primary Assets

Primary Asset Name	*AREA*	*Impact (see Table in the Methodology)*								
		Personnel	Capacity	Performance	Economic	Branding	Regulatory	Environment	Overall Impact	Justification
Input officials' credentials	C	1	4	1	1	4	2	1	3	If this credentials are made public, the validity of the inputted data cannot be trusted.
	I	1	4	4	1	4	4	1	4	If integrity is lost, no one can input the data. The input service is inoperable. High loss of capacity since we can't process any data.
	A	1	4	4	1	4	4	1	4	Idem as integrity loss
GSB / CSB users' credentials	C	1	3	1	1	4	2	1	3	If this credentials are made public, the validity of the results cannot be trusted.
	I	1	3	3	1	4	4	1	4	If integrity is lost, no one can check the input data. The data can be uploaded, but since they cannot be checked, no result can be published: we have moderate loss of capacity.
	A	1	3	3	1	4	4	1	4	Idem as integrity loss
Ballots data input	C	1	1	1	1	4	5	1	3	The election cannot be considered valid, the damage is mainly related to regulatory and branding
	I	1	4	1	1	5	5	1	4	If the input service has been tampered with, we can't conduct a valid election. Furthermore, damaging the integrity of this service can imply a full stop of the system
	A	1	4	1	1	5	5	1	4	If no one can access the input service, we can't conduct the election. The system is completely halted. All systems are operable
Third Party authentication service	C	1	1	1	1	1	1	1	2	This action alone has no impact by following the methodology, but losing the confidentiality of how the service work could lead to the leveraging of vulnerabilities
	I	1	3	3	1	2	1	1	3	If integrity is lost, chairmen cannot authenticate. The system is halted. Also, it is a third party that is at fault, so the Economic, Branding and Regulatory indexes decrease.
	A	1	3	3	1	2	1	1	3	Idem as integrity loss
2 Factor Authentication service	C	1	1	1	1	1	1	1	2	This action alone has no impact by following the methodology, but losing the confidentiality of how the service work could lead to the leveraging of vulnerabilities
	I	1	4	4	1	4	4	1	4	If integrity is lost, no one can check the input data. The data can be uploaded, but since they cannot be checked, the system is partially halted
	A	1	4	4	1	4	4	1	4	Idem as integrity loss
Software Distribution (Virtual Desktop Client)	C	1	1	1	1	1	1	1	1	Software agent can be downloaded but not accessed.
	I	1	4	4	1	4	5	1	5	If the download of the software agent can be tampered, we can have major consequences on capacity and/or performance, and also election results manipulation if the
	A	1	4	4	1	4	4	1	4	If the agent is unaccessible, the system is completely inoperable. At least, election results cannot be manipulated, hence the decrease of the economic, branding and
Result computation	C	1	1	1	1	1	1	1	1	The way in which the computation is made is public
	I	1	5	3	1	5	5	1	5	Modifying the way in which the computation is carried out produces an invalid election result. We have international attention if the produced result is fake
	A	1	5	3	1	4	4	1	4	If the computation is not available, no election result can be produced
Web Application Firewall	C	1	1	1	1	1	1	1	2	Only breaking confidentiality, would have no impact, but knowing what type of traffic is blacklisted can help an adversary at mounting an attack. The inpact is raised at 2
	I	1	3	3	1	4	4	1	4	The WAP is a fundamental security component. An attacker could modify its configuration to block or allow any packet. This can affect the DHV by making it inoperable or by
	A	1	2	3	1	4	4	1	3	If the WAP fails, no packet inspection and forwarding is possible. Communications between Citrix and DHV cannot take place. The system is halted
Diginetwerk routing / communication	C	1	4	1	1	4	2	1	3	If the confidentiality of the communication is broken, also the confidentiality of the credentials is broken. We have similar consequences.
	I	1	4	5	1	4	3	1	5	If the integrity is lost, also availability is lost since we cannot trust the routing to be redirected to the right hosts. All the GSBs can't communicate so, since the entire system is
	A	1	3	5	1	4	3	1	4	Losing availability produces the same effectes as losing integrity. Regulatory and branding are low since the routing is provided by an ISP

GSB LAN to Citrix communicatio n	C	1	2	1	1	4	2	1	2	No impact if the we lose confidentiality fo the way the communication take place
	I	1	2	2	1	4	2	1	3	If the integrity is lost, also availability is lost since we cannot trust the routing to be redirected to the right hosts. The interested GSB is cut off from the network
	A	1	2	2	1	4	2	1	3	Idem as integrity
Import check, approval and signing	C	1	1	1	1	1	1	1	1	The way in which this process is carried out is public
	I	1	2	2	1	5	5	1	3	If the approval process is altered, a non valid result can be approved
	A	1	2	2	1	4	4	1	3	If the approval process is not available, no result can be approved

Figure 3: Impact table

Primary Asset / Supporting Asset	*Input officials' credentials*	*GSB / CSB users' credentials*	*Ballots data input*	Third Party authentication service	2FA authentication service	Software Distribution (Virtual	Result computation	Web Application Firewall	Diginetwerk routing / communicatio	GSB LAN to Citrix communicatio	Inport check, approval and signing	Description / Justification
Third Party Authentication Server Appliances				x								Instance of the TP server. It is assumed that the servers are instantiated outside the Diginetwerk. Without the server instance, the login service is unavailable
Third Party Authentication Database Appliances		x		x								Database used to store the credentials for the setup managers. Whitout this database we can't guarantee authentication
Generic 2FA Server Appliance					x							Instance of the 2FA server used for input officials, GSB and CSB members. Without the server instance, the login service is unavailable
Generic 2FA Database Appliance	x	x			x							Database used to store the credentials for the GSB/CSB members. Whitout this database we can't guarantee authentication
Input Officials	x		x		x							This role is responsible for the input of the counted ballots data. Login through 2FA service is required.
CSB / GSB personeel		x		x	x						x	This users are responsible for checking and approve the imports. Login through 2FA / MFA service is required.
Diginetwerk			x	x	x	x	x		x	x		This is the closed network that hosts the the entire infrastructure. It is a point of failure for many services, since if I can't communicate to the machines, I can't access services nor information
VPN				x								Virtual Private Network used by the HSB users to access the data published by the GSBs
Firewall Appliance								x				Hardware appliance for the WAF
Virtual Desktop Infrastructure (Citrix)			x			x	x				x	Citrix is used to access the DHV environment. Whitout it, the business logic of the DHV env is not accessible
DHV Software			x				x					Software used to compute the election results
Citrix server room(s)				x		x	x	x				Physical place where the server, database, and WAF appliances are placed
GSB PCs			x		x					x		PCs used for connecting to Citrix by the municipalities
Secure Store for GSB PCs			x		x							The secure storing place used to store the GSB PCs
GSB LAN gateway									x	x		Gateways are necessary to ensure communication between the GSB LAN and the virtualization server

Figure 4: Linkage table

Threat Evaluation

Following the identification of the supporting asset, a set of threats and related vulnerabilities were described.

As shown in figure 5, the threats with the highest impacts are the ones tied to the private network and the virtual desktop infrastructure. In particular, those threats are unauthorized wired connections and hyperjacking[9].

These threats were chosen assuming poor access control on the routing equipment of the network and by searching for disrupting incidents for hypervisors.

Another class belongs to the physical realm. More specifically, the threats tied to the physical access to the server rooms and the natural incidents to which the appliances can be exposed were taken into consideration. As can be seen in the table, the impact of these threats is high and cannot be left untreated.

Finally, only the two threats tied to the `GSB LAN gateway` were found to have attenuating circumstances. This is because we are considering the gateway of a single municipality, so the incidents will be limited to that GSB.

Update: following the descriptions of the studied CVEs and related threat scenarios.

Session Hijacking - CVE-2021-22927

This vulnerability affects Citrix Application Delivery Controller (Citrix ADC). An application delivery controller, among its other functions, is responsible for applying security policies. In particular, the infrastructure uses a third-party provider for authentication, entailing the fact that the ADC is configured as a SAML service provider (pre-condition for exploiting the vulnerability).

Threat scenario

To carry out the session fixation attack, an adversary can connect to the application served by the ADC in order to be assigned with a saml-session id. Since the vulnerability states that no privilege are required, we assume that the ADC will assign the id without the need of authentication.

Once the attacker has retrieved the valid id, he/she will need to convince the victim to open a session with the application using the known session id. In the case of a web application, this can be done by convincing a user to open a link in the form of
`https://some.cool.application.com/?SID=SERVER_SET_ID_123456789`.

When the victim performs a login, the adversary will hijack the session using the known session id.[6] Now, the attacker has the privileges of the legitimate user.

Notes on likelihood

Exploiting the vulnerability as in the threat scenario have an high risk of detection and punishment since an attacker needs to employ some social engineering on the victim and probably just an e-mail wouldn't suffice.

Furthermore, the amount of required skills to employ successful social engineering practices is not underestimated.

Reverse Shell Attack - CVE-2022-38652

This vulnerability consists in an insecure deserialization, also called object injection. It affects the software agent of VMWare Hyperic suite, version 5.8.6. In particular, the affected CPE is
`cpe:2.3:a:vmware:hyperic_agent:5.8.6:*:*:*:*:*:*:*`.

For the following threat scenario description, we assume that the vulnerable software runs on the host operating system of the municipality PC.

Threat scenario

As stated in the NVD database[2], to leverage the vulnerability, some not specified authentication material is needed from the VMWare Hyperic Server. To obtain that, the exploit of CVE-2022-38650 is required.

Note that the vulnerabilities afflicting the server and the software agent are of the same type[1]. We assume similar threat scenarios exploiting the two vulnerabilities.

To leverage the vulnerability, an adversary can craft a serialized object `so` starting from a byte stream `bs` controlled by him/her. Subsequently, the attacker sends `so` to the victim that will deserialize it, obtaining `bs`. The deserialized object can contain a call to a function used to run arbitrary code with the privilege of the calling process[10]. For example, in Java such method can be `Runtime.exec()`.

Since this process is often running with `SYSTEM` privileges[2], also the malicious code will inherit `SYSTEM` privileges. At this point an adversary can open an SSH session on any port he/she prefers. As a result, the attacker has completely violated the host machine, granting him/her the power of manipulating the election inputted data.

Notes on likelihood

Even if this vulnerability requires an attacker to follow an attack chain (through CVE-2022-38650 and 38652), the exploit of these two vulnerabilities is assumed to be fairly similar and not too complex (see

also the base metrics). Nonetheless, the means required to execute the attack, the "authentication material" need to be exfiltrated from the server.

Route table poisoning - CVE-2016-7406

Dropbear is a C-written SSH suite consisting of a server and a client [1]. This software is affected by a format string injection caused by bad input sanitization. Further information on format string injection can be found here [2]

Threat scenario

To exploit the vulnerability, during authentication, an attacker can craft a particular username containing a format string parameter (e.g. `% s`) to crash the process or to run arbitrary code with unspecified privileges. We assume the worst case scenario, being execution with root privileges. At this point, an attacker could alter the route table of the gateway. Now, the adversary is able to mount a MITM attack (depending on the cryptographic suite in use in the communication), or just drop the routing table.

Notes on likelihood

Not only the base metrics describe low skills and means requirements, but also modifying the route table and implementing a MITM attack has low chance of detection. Also no need to interact with users and/or acquiring additional knowledge.

[1] https://github.com/mkj/dropbear

[2] https://owasp.org/www-community/attacks/Format_string_attack

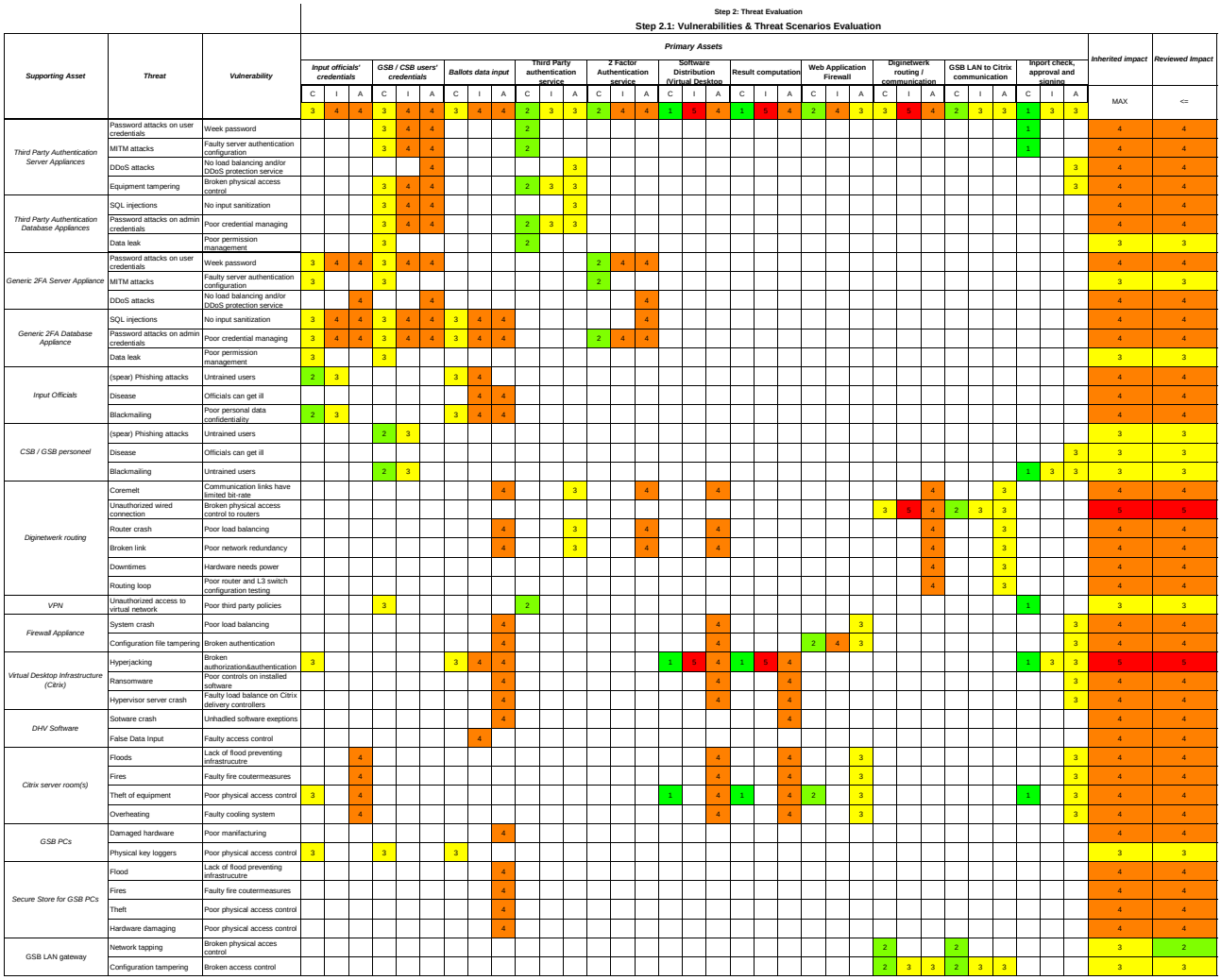

Figure 5: Threat evaluation table

Figure 6 shows how likely it is for an incident tied to a threat to happen. For accidental incidents and natural disasters, only the overall score is assigned.

As can be seen in the table, the majority of the threats with higher impacts like Coremelt are mitigated by their low likelihood. Unfortunately, threats like hyperjacking, equipment theft, and tampering still retain a high likelihood score.

Also, historical events were taken into consideration. In particular, since this system is deployed in the Netherlands, data about flooding was researched[12].

Note that justifications for the likelihood table can be found in the excel file.

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 paricular 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	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 paricular 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	Skills are needed, but it's the information needed to run a phishing
	Disease	Officials can get ill								3	There are great number of input 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	Skills are needed, 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	Physicaly 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, especialy 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,

Figure 6: Threat likelihood table

	Reviewed Impact				
Likelihood	1. No impact, NA	2. Minor	3. Severe	4. Critical	5. Catastrophic
5. Certain	Low	High	High	High	High
4. Very likely	Low	Medium	High	High	High
3. Likely	Low	Low	Medium	High	High
2. Unlikely	Low	Low	Low	Medium	High
1. Very Unlikely	Low	Low	Low	Medium	Medium

Figure 7: Risk table

Risk Evaluation

After having assessed the impact and likelihood scores of the threats, a risk table was adopted.

We believe that the chosen risk table is suitable for our study since, as stated before, we want to ensure a reasonable level of security with a reasonable budget. This is because this system needs to be operational only for a limited time.

In conclusion, we found that the table in figure7 represents a balanced solution.

Having fixed a risk table, we proceeded to evaluate the risk level of the threats, which resulted in a high number of severe threats. The main threats that need mitigation are the ones tied to the most important assets, some of those being

- `unauthorized wired connection` for the private network
- `hyperjacking` for the VDI
- `theft of equipment` for the server rooms and the secure storage of the GSBs
- `router crash` for the private network
- `phishing campaigns` for the input officials and the GSB/CSB personnel

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

Figure 8: Risk evaluation table

Risk Treatment

This part of the assessment aims at proposing a set of pre and post-incident security controls that can be found in figure 9. These controls are needed to lower the impact and the likelihood of an incident.

Regarding the main threats listed in the above section, the following main security controls were proposed

- for `unauthorized wired connections` an intrusion prevention system to reduce the likelihood, and IP blacklist as post-control to reduce impact and avoid APT.
- for `hyperjacking` it is advisable to deploy the latest version of the hypervisor, implement a logical separation between guest and host machines, backup the configuration, and manage the hypervisor on a different port than the one used for hypervisor-guest communication[11]. As post-controls, we can try and reset the admin credential, and restore the virtualization server with its backup, but if the access control is broken, then disaster recovery is needed.
- for `theft of equipment` the pre-controls consist of installing CCTV cameras, biometrical access control, and log personnel access. Since it's not reasonable to ask a municipality to install biometrical access control on a room that is used only when we are near the elections, we substituted this with a security officer.[8]
- for `router crashes` the main mitigations consist of implementing VRRP (Virtual Router Redundancy Protocol) [5] and configuration backup and restore when needed.
- finally, for `phishing campaigns` we need to train the personnel and implement anti-spam software on mail agents and SMTP servers to reduce the likelihood.

At the end of this step, no threats with high risk rating remained.

Update:

Session Hijacking - CVE-2021-22927

Citrix systems Inc. has already released an official patch with a reference guide on how to configure SAML. For this reason the vulnerability can be removed by upgrading the Citrix ADC software to version `13.0-82.41` or later, and by following the official configuration guide. [3]

As a result, the impact is nulled.

Reverse Shell Attack - CVE-2022-38652

It is stated in the vulnerability description that the affected products are in their EOL (End-of-Life) stage. No official patches or workarounds are available. As a first approach, the deployment of a DPI firewall was taken into consideration. More specifically, the goal was to whitelist only the necessary ports in order to block the instantiation of sockets used to expose the reversed shell.

Unfortunately, not only this mitigation is too shallow since it only modifies the MAV metric, but also it can be bypassed. In fact, if an attacker has `SYSTEM` privileges on the victim machine, he/she could kill a process running on a whitelisted port and start an SSH session on that socket. Furthermore, to break the deep packet inspection, an adversary could tunnel the SSH session through a full TLS connection.[7]

The vulnerability is reported to exists only in the software version for Windows systems. We suggest two approaches that depends on the production environment:

- **deploy the software on a container running a Linux based OS**; this can be done by setting docker option `--ipc=host`. Note that this option drops the security requirements of the container and need to be tested.
- **replace Windows host with a Linux based OS**; this solution is more time consuming but it's the safest since it has been confirmed that the vulnerability does not exists in this environment.

[3] https://support.citrix.com/article/CTX316577/citrix-application-delivery-controller-and-citrix-gateway-saml-configuration-reference-guide

To comply with our strict security policy, the second suggested solution is strongly advised as it surely nulls the impact of the threat.

Route table poisoning - CVE-2016-7406

An official patch is publicly available. We suggest upgrading to version 2016.74 or higher.[4]

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					

				Check audit for misconduct					
Diginetwerk	*Coremelt*	*Communication links have limited bit-rate*	Implement stronger link redundancy	Enforce a probabilistic packages drop in order to punish aggressive flows	4	2	3	1	LOW
			Monitor traffic to detect anomalies						
	Unauthorized wired connection	*Broken physical access control to routers*	Install intrusion prevention system	Check logs of databases and authentication services for malicious	5	3	4	2	MEDIUM
				Disaster recovery					
				Blacklist IP					
	Router crash	*Poor load balancing*	Implement VRRP or proprietary alternative	Automated switch to backup router through VRRP	4	3	1	3	LOW
			Configuration backup	Restore router with backed up configuration					
	Broken link	*Poor network redundancy*	Implement stronger link redundancy	If the link is broken and there is no redundancy, recovery plan is needed	4	3	4	2	MEDIUM
	Downtimes	*Hardware needs power*		Disaster recovery	4	2	4	2	MEDIUM
	Routing loop	*Poor router and L3 switch configuration testing*	Backup configuration	Reset and restore configuration	4	3	3	2	LOW
			Test routers and L3 switch configurations						
VPN	Unauthorized access to virtual network	Poor third party policies	Adopt zero trust model on the perimeter of the VPN tunneling	Disaster recovery	3	4	3	3	MEDIUM
			Check incident history of third party provider to select						
Firewall appliance	System crash	*Poor load balancing*	Install firewall with that supports the required bitrate	Reset firewall with backed up configuration	4	3	2	2	LOW
			Backup firewall configuration						
	Configuration file tampering	*Broken authentication*	Backup firewall configuration	Reset firewall with backed up configuration	4	4	4	2	MEDIUM
			Deploy with latest firmware	Disaster recovery					
			Check for vulnerabilities and official fixes / workarounds						
Virtual Desktop Infrastructure (Citrix)	Hyperjacking	Broken authorization&authentication	Deploy latest version of the hypervisor software	Reset admin credentials	5	4	4	2	MEDIUM
			Configure hard logical separation between hypervisor and guest OSs	Backup hijacked hypervisor image for forensics					
			Backup the hypervisor configuration	Restore configuration					
			Keep hypervisor management traffic separated from users traffic	Disaster recovery					
	Ransomware	Poor controls on installed software	Use approved removable drives only	Backup hypervisor image for forensics	4	4	2	3	LOW
			Backup the hypervisor configuration	Restore hypervisor configuration					
			Keep logs of installation requests	Re-distribute software					
			Deploy latest version of the hypervisor software and latest version of the guest OSs	Re-deploy guest machines					
	Hypervisor server crash	Faulty load balance on Citrix delivery controllers	Test the virtualization server configuration	Restore hypervisor configuration	4	3	3	2	LOW
			Backup the hypervisor configuration	Re-deploy guest machines					
DHV Software	Sotware crash	Unhadled software exeptions	Perform unit testing	Disaster recovery	4	2	4	1	MEDIUM
	False Data Input	Faulty access control	Adopt least priviledge access control	Disaster recovery	4	3	4	2	MEDIUM
			System logs and audit						
Citrix server room(s)	Floods	Lack of flood preventing infrastrucutre	Avoid using rooms with water pipes behind walls	Disaster recovery	4	3	4	2	MEDIUM
			Define flood response roles and train personeel						
			Put server room on second floor or above						
	Fires	Faulty fire countermeasures	Define fire response roles and train personeel	Disaster recovery	4	2	4	1	MEDIUM
			Install fire suppression system with inert gas						
	Theft of equipment	Poor physical access control	Adopt CCTV cameras	If the equipment has a backup appliance, use backup	4	4	4	1	MEDIUM
			Use biometrical access control	Disaster recovery					
			Audit personeel access to server room						
	Overheating	Faulty cooling system	Install temperature sensors	If the equipment has a backup appliance, use backup	4	3	4	1	MEDIUM
			Adopt enclosed hot aisles	Disaster recovery					
			Switch off unnecessary and reduntant hardware when the temperature raises up						
			Perform due maintenance on the AC						
GSB PCs	Damaged hardware	Poor manifacturing	Test systems before deploying	If the equipment has a backup appliance, use backup	4	3	3	1	LOW
			Buy some backup PCs	Disaster recovery					
	Physical key loggers	Poor physical access control	Check I/O hardware before deploying	Check for misconduct tied to user credentials	3	4	3	2	LOW
				Reset users credential					
Secure Store for GSB PCs	Flood	Lack of flood preventing infrastrucutre	Define flood response roles and train personeel	Disaster recovery	4	3	4	2	MEDIUM
			Avoid using rooms with water pipes behind walls						
			Put store room on second floor or above						
	Fires	Faulty fire countermeasures	Install fire alarms	Disaster recovery	4	2	4	1	MEDIUM
			Define fire response roles and train personeel						
			Buy inert fire estinguishers						
	Theft	Poor physical access control	Audit personeel access to secure room	If the equipment has a backup appliance, use backup	4	4	4	1	MEDIUM
			Put security officer at entry point	Disaster recovery					
			Adopt CCTV cameras						
	Hardware damaging	Poor physical access control	Audit personeel access to secure room	If the equipment has a backup appliance, use backup	4	4	4	1	MEDIUM
			Put security officer at entry point	Disaster recovery					
			Adopt CCTV cameras						
GSB LAN gateway	Network tapping	Broken physical access control	Audit personeel access to secure room	Reset passwords for interested GSB	2	4	1	1	LOW
			Put security officer at entry point	Remove network tap					
			Adopt CCTV cameras						
	Configuration tampering	Broken access control	Backup gateway configuration	Disaster recovery	3	4	3	2	LOW
			Deploy with latest firmware						
			Check for vulnerabilities and official fixes / workarounds						

Figure 9: Risk treatment

Bibliography

[1] National Vulnerability Database. *CVE-2022-38650*. https://nvd.nist.gov/vuln/detail/CVE-2022-38650. Accessed 2023-06-14. NIST, 2022.

[2] National Vulnerability Database. *CVE-2022-38652*. https://nvd.nist.gov/vuln/detail/CVE-2022-38652. Accessed 2023-06-14. NIST, 2022.

[3] Miriam le Fevre et al. *SecRAM 2.0 - Security Risk Assessment methodology for SESAR 2020*. https://www.sesarju.eu/sites/default/files/documents/transversal/SESAR%202020%20-%20Security%20Reference%20Material%20Guidance.pdf. Accessed 2023-05-14. SESAR, 2022.

[4] Inc. Gentoo Foundation. *Dropbear: Multiple vulnerabilities*. https://security.gentoo.org/glsa/201702-23. Accessed 2023-06-14. Gentoo Foundation, Inc., 2017.

[5] Huawei. *What Is VRRP?* https://info.support.huawei.com/info-finder/encyclopedia/en/VRRP.html. Accessed 2023-05-14. Huawei Technologies Co., Ltd., 2022.

[6] Mitja Kolsek. "Session fixation vulnerability in web-based applications". In: *ACROS Security, https://chabloz.eu/files/attaqueFixation.pdf* (2002).

[7] Dmitriy Kuptsov. *Bypassing Deep Packet Inspection: Tunneling Traffic Over TLS VPN*. https://www.linuxjournal.com/content/bypassing-deep-packet-inspection-tunneling-traffic-over-tls-vpn. Accessed 2023-06-14. Slashdot Media, LLC, 2021.

[8] Ophtek. *How Do You Secure a Server Room?* https://ophtek.com/how-do-you-secure-a-server-room/. Accessed 2023-05-14. Ophtek, 2021.

[9] Katie Rees. *What Is a Hyperjacking Attack and Are You at Risk?* https://www.makeuseof.com/what-is-hyperjacking-attack/. Accessed 2023-05-14. MAKE USE OF, 2022.

[10] Imen Sayar et al. "An In-Depth Study of Java Deserialization Remote-Code Execution Exploits and Vulnerabilities". In: *ACM Trans. Softw. Eng. Methodol.* 32.1 (Feb. 2023). ISSN: 1049-331X. DOI: 10.1145/3554732. URL: https://doi.org/10.1145/3554732.

[11] Telelink. *Hyperjacking*. https://web.archive.org/web/20150227174207/http://itsecurity.telelink.com/hyperjacking/. Accessed 2023-05-14. Telelink, 2014.

[12] WAGENINGEN University. *Flooding - Dossier*. https://www.wur.nl/en/dossiers/file/flooding.html. Accessed 2023-05-14. WAGENINGEN University, 2021.