



**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

<b>Executive Summary</b>	<b>2</b>
<b>Target of evaluation</b>	<b>3</b>
<b>Summary of findings</b>	<b>4</b>
<b>Risk Analysis</b>	<b>5</b>
Impact assessment . . . . .	5
Supporting Asset Identification & Valuation . . . . .	6
Threat Evaluation . . . . .	8
Risk Evaluation . . . . .	13
Risk Treatment . . . . .	15

# 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 rely on a third-party ISP infrastructure.

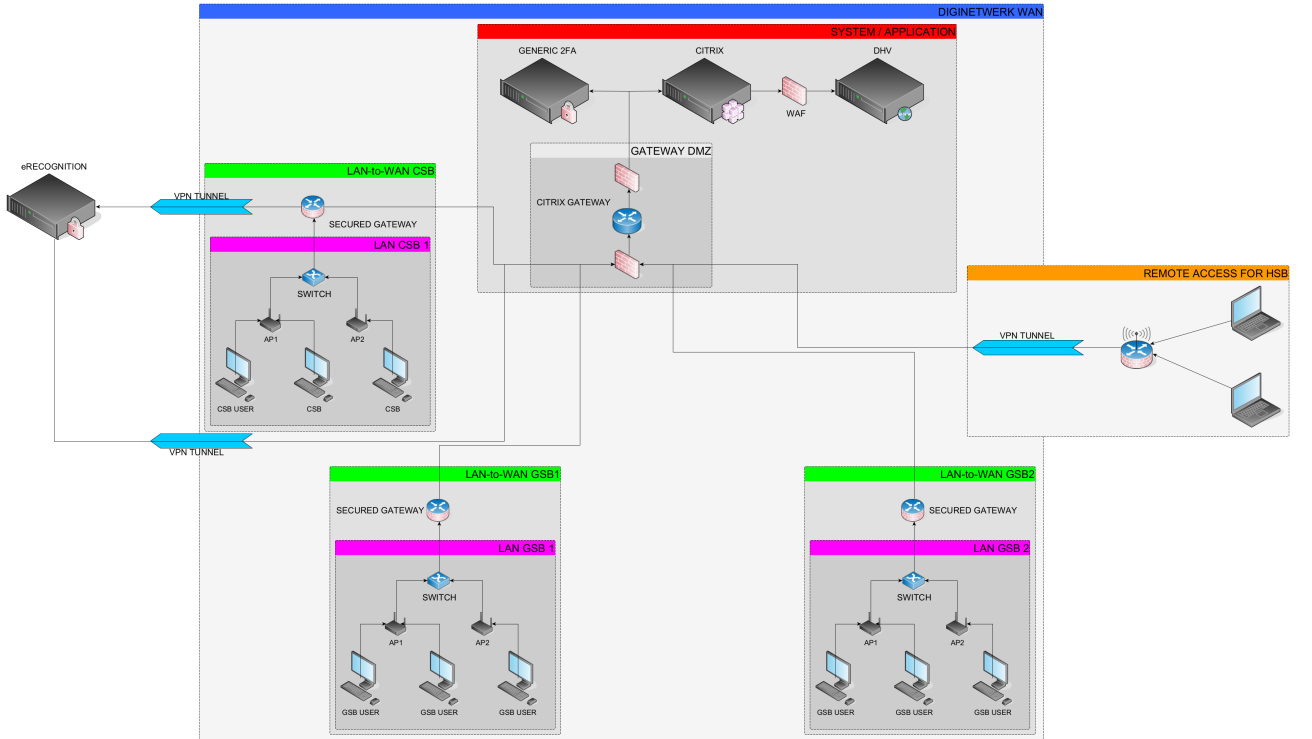


Figure 1: High-level assumed network topology

# 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 software 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 results, 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)								Justification
		Personnel	Capacity	Performance	Economic	Branding	Regulatory	Environment	Overall Impact	
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 agent is unaccessible, the system is completely inoperable. At least, election results cannot be manipulated, hence the decrease of the economic, branding and
	A	1	4	4	1	4	4	1	4	
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 impact 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 communication	C	1	2	1	1	4	2	1	2	No impact if the we lose confidentiality to 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	Digineverk routing / communicatio	GSB LAN to Citrix communication	Import 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 Digineverk. 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. Without 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. Without 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 / MFA 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.
Digineverk			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. Without 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[8].

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.[5] 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[9]. 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.

			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			Diginetwork routing / communication			GSB LAN to Citrix communication			Import 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	
			3	4	4	3	4	4	3	4	4	2	3	3	2	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	MAX	<<
Third Party Authentication Server Appliances	Password attacks on user credentials	Weak password				3	4	4				2																								4	4	
	MITM attacks	Faulty server authentication configuration				3	4	4				2																								4	4	
	DDoS attacks	No load balancing and/or DDoS protection service						4					5																				3	4	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	Weak 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	
	SQL injections	No input sanitization	3	4	4	3	4	4	3	4	4																									4	4	
Generic 2FA Database Appliance	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 personnel	(spear) Phishing attacks	Untrained users				2	3																												3	3		
	Disease	Officials can get ill																																3	3	3	3	
	Blackmailing	Untrained users				2	3																												3	3		
	Correat	Communication links have limited bit-rate								4			3			4																				4	4	
Diginetwork routing	Unauthorized wired connection	Broken physical access control to routers																									3	4	4	2	3	3				5	5	
	Router crash	Poor load balancing								4			3			4			4																4	4		
	Broken link	Poor network redundancy								4			3			4																				4	4	
	Downtimes	Hardware needs power																																			4	4
VPN	Routing loop	Poor router and L3 switch configuration testing																																		4	4	
	Unauthorized access to virtual network	Poor third party policies				3						2																								3	3	
Firewall Appliance	System crash	Poor load balancing								4									4																3	4	4	
	Configuration file tampering	Broken authentication								4																2	4	3							3	4	4	
Virtual Desktop Infrastructure (Citrix)	Hyperjacking	Broken authorization/authentication	3						3	4	4					1	4	4	1	4	4															5	5	
	Ransomware	Poor controls on installed software																	4															3	4	4		
DHV Software	Hypervisor server crash	Faulty load balance on Citrix delivery controllers																	4																3	4	4	
	Software crash	Unhandled software exceptions																																		4	4	
	False Data Input	Faulty access control								4																										4	4	
Citrix server room(s)	Floods	Lack of flood preventing infrastructure				4													4															3	4	4		
	Fires	Faulty fire countermeasures				4													4															3	4	4		
	Theft of equipment	Poor physical access control	3			4													4	4	4	2	3											3	4	4		
	Overheating	Faulty cooling system				4													4																3	4	4	
GSB PCs	Damaged hardware	Poor manufacturing																																		4	4	
	Physical key loggers	Poor physical access control	3			3			3																											3	3	
	Flood	Lack of flood preventing infrastructure																																		4	4	
	Fires	Faulty fire countermeasures																																		4	4	
Secure Store for GSB PCs	Theft	Poor physical access control																																		4	4	
	Hardware damaging	Poor physical access control																																		4	4	
	Network tapping	Broken physical access control																																		3	2	
	Configuration tampering	Broken access control																																		3	3	

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[11].

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							Overall Likelihood (2.2)	Justification
			Skills	Means	Opportunity	Profit	Attention	Impunity	Detection		
Third Party Authentication Server Appliances	Password attacks on user credentials	Weak password	3	4	5	1	4	4	3	4	Password attacks are really common, especially in systems that have strong authentication and require particular means or skills. This entail an high
	MITM attacks	Faulty server authentication configuration	4	4	3	1	4	4	4	4	DDoS attacks require a great numbers of slaves that need to be bought or infected
	DDoS attacks	No load balancing and/or DDoS protection service	2	2	5	1	5	4	2	3	High chance of punishment and detection
	Equipment tampering	Broken physical access control	3	3	5	1	5	2	2	3	Common attack, low skills needed, low chance of punishment and detection if
Third Party Authentication Database Appliances	SQL injections	No input sanitization	4	4	5	1	5	4	3	4	Password attacks are really common, especially in systems that have strong
	Password attacks on admin credentials	Poor credential managing	3	4	5	1	5	4	4	4	need for or skills and means to convince someone to leak information.
	Data leak	Poor permission management	1	1	2	1	5	2	2	2	Password attacks are really common, especially in systems that have strong
Generic 2FA Server Appliance	Password attacks on user credentials	Weak 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	need for or skills and means to convince someone to leak information.
	DDoS attacks	No load balancing and/or DDoS protection service	2	2	5	1	5	4	2	3	Password attacks are really common, especially in systems that have strong
	SQL injections	No input sanitization	4	4	5	1	5	4	3	4	need for or skills and means to convince someone to leak information.
Generic 2FA Database Appliance	Password attacks on admin credentials	Poor credential managing	3	4	5	1	5	4	4	4	Skills are needed, but it's the information needed to run a phishing
	Data leak	Poor permission management	5	2	2	1	5	2	3	3	there are great number of impersonator, there is a reasonable possibility that
	(spear) Phishing attacks	Untrained users	3	4	5	1	4	3	4	4	less probable of phishing, since it's usually harder to obtain information to
Input Officials	Disease	Officials can get ill								3	Skills are needed, but it's the information needed to run a phishing
	Blackmailing	Poor personal data confidentiality	3	2	5	1	4	3	3	3	there are great number of impersonator, there is a reasonable possibility that
	(spear) Phishing attacks	Untrained users	3	5	5	1	4	3	4	4	less probable of phishing, since it's usually harder to obtain information to
CSB / GSB personeel	Disease	Officials can get ill								2	Skills are needed, but it's the information needed to run a phishing
	Blackmailing	Untrained users	3	2	5	1	4	3	3	3	there are great number of impersonator, there is a reasonable possibility that
	Coremelt	Communication links have limited bit-rate	1	2	5	1	5	4	1	2	less probable of phishing, since it's usually harder to obtain information to
Diginetwerk	Unauthorized wired connection	Broken physical access control to routers	4	3	5	1	5	2	2	3	Skills are needed, but it's the information needed to run a phishing
	Router crash	Poor load balancing								3	there are great number of impersonator, there is a reasonable possibility that
	Broken link	Poor network redundancy								2	less probable of phishing, since it's usually harder to obtain information to
	Downtimes	Hardware needs power								2	Skills are needed, but it's the information needed to run a phishing
	Routing loop	Poor router and L3 switch configuration testing								3	there are great number of impersonator, there is a reasonable possibility that
VPN	Unauthorized access to virtual network	Poor third party policies	2	3	5	1	5	4	4	4	less probable of phishing, since it's usually harder to obtain information to
Firewall appliance	System crash	Poor load balancing								3	Skills are needed, but it's the information needed to run a phishing
	Configuration file tampering	Broken authentication	4	3	5	1	4	3	3	4	there are great number of impersonator, there is a reasonable possibility that
Virtual Desktop Infrastructure (Citrix)	Hyperjacking	Broken authorization&authentication	3	3	5	1	5	4	2	4	less probable of phishing, since it's usually harder to obtain information to
	Ransomware	Poor controls on installed software	3	3	5	5	5	3	2	4	Skills are needed, but it's the information needed to run a phishing
	Hypervisor server crash	Faulty load balance on Citrix delivery controllers								3	there are great number of impersonator, there is a reasonable possibility that
DHV Software	Software crash	Unhadled software exeptions								2	less probable of phishing, since it's usually harder to obtain information to
	False Data Input	Faulty access control	3	2	3	1	5	4	3	3	Skills are needed, but it's the information needed to run a phishing
Citrix server room(s)	Floods	Lack of flood preventing infrastrucutre								3	there are great number of impersonator, there is a reasonable possibility that
	Fires	Faulty fire coutermeasures								2	less probable of phishing, since it's usually harder to obtain information to
	Theft of equipment	Poor physical access control	5	5	5	3	4	2	1	4	Skills are needed, but it's the information needed to run a phishing
	Overheating	Faulty cooling system								3	there are great number of impersonator, there is a reasonable possibility that
GSB PCs	Damaged hardware	Poor manufacturing								3	less probable of phishing, since it's usually harder to obtain information to
	Physical key loggers	Poor physical access control	4	4	5	1	5	2	2	4	Skills are needed, but it's the information needed to run a phishing
Secure Store for GSB PCs	Flood	Lack of flood preventing infrastrucutre								3	there are great number of impersonator, there is a reasonable possibility that
	Fires	Faulty fire coutermeasures								2	less probable of phishing, since it's usually harder to obtain information to
	Theft	Poor physical access control	5	5	5	3	4	2	1	4	Skills are needed, but it's the information needed to run a phishing
	Hardware damaging	Poor physical access control	5	5	5	1	4	2	1	4	there are great number of impersonator, there is a reasonable possibility that
GSB LAN gateway	Network tapping	Broken physical acces control	4	4	5	1	4	2	2	4	less probable of phishing, since it's usually harder to obtain information to
	Configuration tampering	Broken access control	3	5	5	1	4	3	3	4	Skills are needed, but it's the information needed to run a phishing

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	Weak 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	Weak 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 personnel	(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 manufacturing	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[10]. 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.[7]
- for **router crashes** the main mitigations consist of implementing VRRP (Virtual Router Redundancy Protocol) [4] 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.<sup>1</sup>

As a result, the impact is nulled.

### Session Hijacking - CVE-2021-22927

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 full a TLS connection.[6]

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.

---

<sup>1</sup><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.

#### 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 assignment	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 backup					
	Password attacks on admin credentials	Poor credential managing	Enforce strong password assignment	Block admin account	4	4	3	3	MEDIUM
			Backup database configuration	Notify admin and enforce password reset					
	Data leak	Poor permission management	Password hashing + salting	If needed restore database configuration and users data	3	2	2	2	LOW
Setup transaction audit for the database			Block accounts						
Generic 2FA Server Appliance	Password attacks on user credentials	Week password	Enforce strong password assignment	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 backup					
	Password attacks on admin credentials	Poor credential managing	Enforce strong password assignment	Block admin account	4	4	3	3	MEDIUM
			Backup database configuration	Notify admin and enforce password reset					
	Data leak	Poor permission management	Password hashing + salting	If needed restore database configuration and users data	3	3	2	2	LOW
Setup transaction audit for the database			Block accounts						
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
CSB / GSB personnel	(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					

Critical Assets for Infrastructure									
Diginetwork	Coremelt	Communication links have limited bit-rate	Implement stronger link redundancy Monitor traffic to detect anomalies	Enforce a probabilistic packages drop in order to punish aggressive flows	4	2	3	1	LOW
	Unauthorized wired connection	Broken physical access control to routers	Install intrusion prevention system	Check logs of databases and authentication services for malicious Disaster recovery Blacklist IP	5	3	4	2	MEDIUM
	Router crash	Poor load balancing	Implement VRRP or proprietary alternative Configuration backup	Automated switch to backup router through VRRP Restore router with backed up configuration	4	3	1	3	LOW
	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 Test routers and L3 switch configurations	Reset and restore configuration	4	3	3	2	LOW
VPN	Unauthorized access to virtual network	Poor third party policies	Adopt zero trust model on the perimeter of the VPN tunneling Check incident history of third party provider to select	Disaster recovery	3	4	3	3	MEDIUM
Firewall appliance	System crash	Poor load balancing	Install firewall with that supports the required bitrate Backup firewall configuration	Reset firewall with backed up configuration	4	3	2	2	LOW
	Configuration file tampering	Broken authentication	Backup firewall configuration Deploy with latest firmware Check for vulnerabilities and official fixes / workarounds	Reset firewall with backed up configuration Disaster recovery	4	4	4	2	MEDIUM
Virtual Desktop Infrastructure (Citrix)	Hyperjacking	Broken authorization&authentication	Deploy latest version of the hypervisor software Configure hard logical separation between hypervisor and guest OSs Backup the hypervisor configuration Keep hypervisor management traffic separated from users traffic	Reset admin credentials Backup hijacked hypervisor image for forensics Restore configuration Disaster recovery	5	4	4	2	MEDIUM
	Ransomware	Poor controls on installed software	Use approved removable drives only Backup the hypervisor configuration Keep logs of installation requests Deploy latest version of the hypervisor software and latest version of the guest OSs	Backup hypervisor image for forensics Restore hypervisor configuration Re-distribute software Re-deploy guest machines	4	4	2	3	LOW
	Hypervisor server crash	Faulty load balance on Citrix delivery controllers	Test the virtualization server configuration Backup the hypervisor configuration	Restore hypervisor configuration Re-deploy guest machines	4	3	3	2	LOW
DHV Software	Software crash	Unhadled software exceptions	Perform unit testing	Disaster recovery	4	2	4	1	MEDIUM
	False Data Input	Faulty access control	Adopt least privilege access control System logs and audit	Disaster recovery	4	3	4	2	MEDIUM
Citrix server room(s)	Floods	Lack of flood preventing infrastructure	Avoid using rooms with water pipes behind walls Define flood response roles and train personnel Put server room on second floor or above	Disaster recovery	4	3	4	2	MEDIUM
	Fires	Faulty fire countermeasures	Define fire response roles and train personnel Install fire suppression system with inert gas	Disaster recovery	4	2	4	1	MEDIUM
	Theft of equipment	Poor physical access control	Adopt CCTV cameras Use biometrical access control Audit personnel access to server room	If the equipment has a backup appliance, use backup Disaster recovery	4	4	4	1	MEDIUM
	Overheating	Faulty cooling system	Install temperature sensors Adopt enclosed hot aisles Switch off unnecessary and redundant hardware when the temperature raises up Perform due maintenance on the AC	If the equipment has a backup appliance, use backup Disaster recovery	4	3	4	1	MEDIUM
GSB PCs	Damaged hardware	Poor manufacturing	Test systems before deploying Buy some backup PCs	If the equipment has a backup appliance, use backup Disaster recovery	4	3	3	1	LOW
	Physical key loggers	Poor physical access control	Check I/O hardware before deploying	Check for misconduct tied to user credentials Reset users credential	3	4	3	2	LOW
Secure Store for GSB PCs	Flood	Lack of flood preventing infrastructure	Define flood response roles and train personnel Avoid using rooms with water pipes behind walls Put store room on second floor or above	Disaster recovery	4	3	4	2	MEDIUM
	Fires	Faulty fire countermeasures	Install fire alarms Define fire response roles and train personnel Buy inert fire estinguishers	Disaster recovery	4	2	4	1	MEDIUM
	Theft	Poor physical access control	Audit personnel access to secure room Put security officer at entry point Adopt CCTV cameras	If the equipment has a backup appliance, use backup Disaster recovery	4	4	4	1	MEDIUM
	Hardware damaging	Poor physical access control	Audit personnel access to secure room Put security officer at entry point Adopt CCTV cameras	If the equipment has a backup appliance, use backup Disaster recovery	4	4	4	1	MEDIUM
GSB LAN gateway	Network tapping	Broken physical access control	Audit personnel access to secure room Put security officer at entry point Adopt CCTV cameras	Reset passwords for interested GSB Remove network tap	2	4	1	1	LOW
	Configuration tampering	Broken access control	Backup gateway configuration Deploy with latest firmware Check for vulnerabilities and official fixes / workarounds	Disaster recovery	3	4	3	2	LOW

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] Huawei. *What Is VRRP?* <https://info.support.huawei.com/info-finder/encyclopedia/en/VRRP.html>. Accessed 2023-05-14. Huawei Technologies Co., Ltd., 2022.
- [5] Mitja Kolsek. “Session fixation vulnerability in web-based applications”. In: *ACROS Security*, <https://chabloz.eu/files/attaqueFixation.pdf> (2002).
- [6] 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.
- [7] Ophtek. *How Do You Secure a Server Room?* <https://ophtek.com/how-do-you-secure-a-server-room/>. Accessed 2023-05-14. Ophtek, 2021.
- [8] 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.
- [9] 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>.
- [10] Telelink. *Hyperjacking*. <https://web.archive.org/web/20150227174207/http://itsecurity.telelink.com/hyperjacking/>. Accessed 2023-05-14. Telelink, 2014.
- [11] WAGENINGEN University. *Flooding - Dossier*. <https://www.wur.nl/en/dossiers/file/flooding.html>. Accessed 2023-05-14. WAGENINGEN University, 2021.