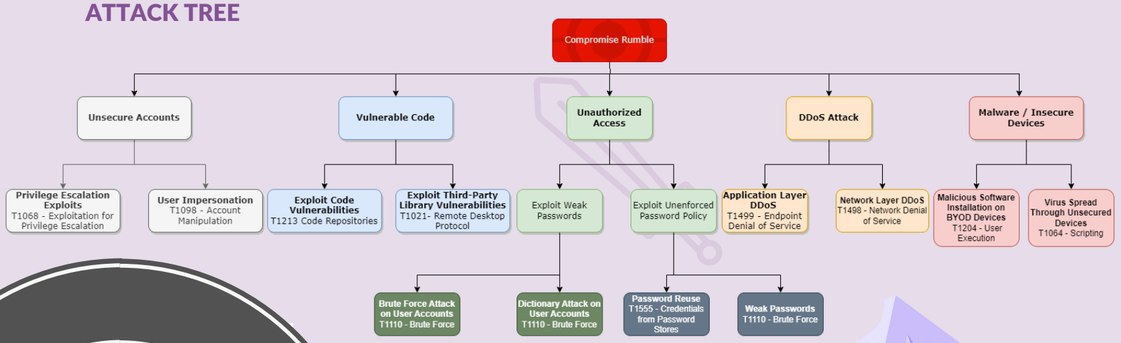
ATTACK TREE



RISKS & THEIR LIKELIHOOD

Risks	Likelihood
Passwords	81% of all data reaches are due to poor password management (Verizon, 2023)
DDoS Attack	20% of companies with more than 50 employees experience DDoS attack (Kaspersky Lab, 2015)
Virus/ Insecure Devices	16.5% experience a malware attack (Chen, 2021)
Vulnerable code	19% of software contains critical vulnerabilities (Palatty, 2023)
Unsecure accounts	The average rate of a broken access control is 3.81% (OWASP, 2021)

USABILITY

The ISO 9241-11 is used to determine the usability in the table below. It recommends to score the solutions based on effectiveness, efficiency and satisfaction.

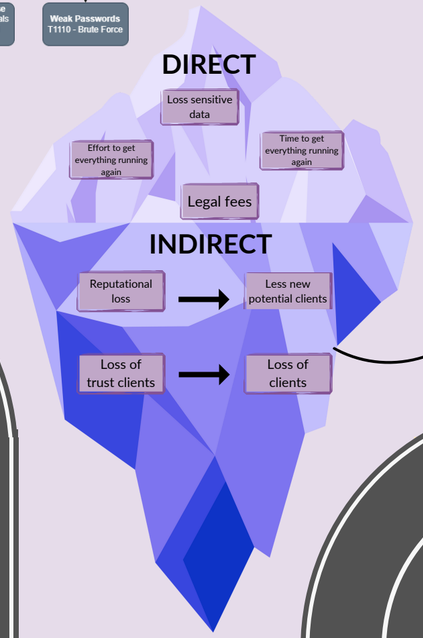
	Password Manager	Principle of Least Privilege	Device Security Policies for BYOD devices	Multi-factor Authenticator	Agile Workflow	Web Application Firewall	Hardware Firewall
Effectiveness	High	High	High	Very High	Low to Moderate	High	High
Efficiency	Moderate	High	Moderate	High	Moderate	Moderate	Low to Moderate
Satisfaction	Moderate to High	Moderate to High	Moderate to High	Moderate to High	Moderate to High	Moderate to High	Moderate to High

EXPLANATION USABILITY

In the table on the right, more information can be found on what the results in the table above are based on.

	Effectiveness	Efficiency	Satisfaction
Password Manager	Users can effectively manage and use complex passwords without the need to remember them, improving overall security.	Although there may be an initial investment of time for users to adapt, the long-term efficiency is significant as it simplifies password management.	Users may initially find it an additional step, but once accustomed, they appreciate the enhanced security and convenience.
Principle of Least Privilege	Least privilege effectively limits access to necessary functions, reducing the risk of unauthorized actions.	Properly configured least privilege reduces the risk of errors and unauthorized access, making system usage more efficient.	Users may initially find it restrictive, but as they understand the security benefits, satisfaction increases. The comfort level improves with clear communication and training.
Device security policies for BYOD Devices	MDM enhances control and security over BYOD devices, reducing the risk of unauthorized access and data breaches.	The initial setup and ongoing management may require some effort, but the increased security offsets the impact on efficiency.	Administrators appreciate the security benefits of MDM, while users may find it a reasonable trade-off for the increased protection of their devices and data.
Implement Multi-Factor Authentication (MFA)	MFA significantly enhances security by requiring multiple forms of authentication, reducing the risk of unauthorized access.	While MFA adds an extra step, the additional security outweighs the minimal impact on efficiency.	Users generally appreciate the enhanced security provided by MFA once they understand its benefits. The initial inconvenience may be offset by increased peace of mind.
Agile Workflow	It doesn't reduce the chances of having vulnerable code/ unsecure account, but it helps in case it does happen.	There are little resources needed to organize a SCRUM meeting. It only takes 20 minutes of the day to provide each other updates about their projects, while it can help in solving attacks faster.	Although it requires some time of the day, it can improve the communication and keep each other informed.
Web application firewall	Web application firewalls helps filter and blocking malicious attacks and preventing the system becoming unavailable.	There is already a web application firewall installed, however it needs some adjustment to work efficiently.	It is generally user-friendly and easy to manage.
Hardware firewall	Hardware firewalls helps filter and blocking malicious attacks and preventing the system becoming unavailable.	The initial time investment already has been put in as it is already installed in.	It is generally user-friendly and easy to manage.

DIRECT AND INDIRECT LOSSES



The indirect costs are especially important for Rumble. Since Rumble is a **small** and **fast-growing** company, a reputational loss and a loss of trust might potentially stop their growth and be **fatal** for the company.

1 COMPANY

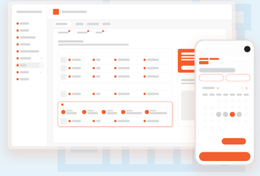
RUMBLE

Naaldwijk

Software development company catering to the automotive industry.

Aims to simplify claim and repair management vehicles.

Usage-based subscription on their SaaS platform *RumbleDirect*, with a montly fee per vehicle dossier.



Small sized company: <10 Full Time Employees

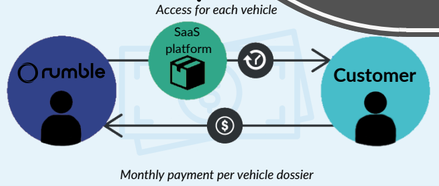
Exponential growth company in the past few months shows the urgent need for stricter security measures.

ROLE ICT

ICT plays a big role in Rumble. ICT is mostly used for the following activities:

- **Creating software applications** is the main activity of Rumble.
- **Communication** with the clients and other colleagues, via meetings and email.
- **Client data** for the assignments is stored in a database.

REVENUE MODEL



2 THREATS

3 SOLUTIONS

DEFENSES AND THEIR COSTS

COST CALCULATIONS

Cost calculations are based on the following numbers:

- **€30/hour** is the average company salary
- There are **10 full-time workers** in the company

PASSWORD

Multi-factor authentication (MFA)

- Force employees to use a multi-factor authenticator
- Costs: Relatively 0
- Impact: 99.9% less likely to be compromised (Luchenko & Semenova, 2023)

Password Manager

- **Onepassword** already installed in the company, but **not** enforced for all employees.
- Costs: takes 1 day to set up. This will cost €240/employee. And around €2000 in total. + €5/month per password

DDOS & VIRUS ATTACKS

Web application firewall

- **Sucuri** is already installed on development server.
- Costs: €2000
- Impact: Lower chances DDos and virus attacks.

Hardware firewall

- Current defenses need to be upgraded
- Costs: free but setting up costs were €5000.
- Impact: Lower chances DDos and virus attacks.

Antivirus and keeping systems up-to-date

- **Device Policy (in combination with SBOM)** would **enforce** this.
- Costs: €2000-3000.
- Impact: **Update** and **overview** of **software** on all **Windows** device.

VULNERABLE CODE & UNSECURE ACCOUNTS

Principle of minimum permission

- **Only** giving access to sensitive data if the employee **needs** the data.
- Costs: Takes 1 day to set up. This will cost €240.
- Impact: less likely to lose sensitive data in case an account is hacked

Agile workflow

- Part of an agile workflow, enforces an **update** meeting **every** day, improving communications.
- Costs: 20 minutes a day per employee. This will cost €100/day
- Impact: being able to reply **faster** and **more adequately** in case of an **attack**.

4 IMPLEMENTATION

COSTS VS IMPACT

The cost and impact is all based on comparison with other solutions

	Impact	Costs
MFA	High	Low
Password Manager	Medium	High
Principle of minimum permission	Low	Low
SCRUM	Medium	High
Web Application Firewall	Medium	Medium
Hardware Firewall	High	High
Device Policy	High	Medium

GROUP 10

Quinten van Breugel

Narcisa Dobre

David Galati

Lena de Kraker

Cheng Qi Wang

UNIVERSITY OF TWENTE. rumble