Vulnerability Assessment

BetterBe - Transforming automotive leasing worldwide

UT Team Group 2 / 01. 01. 2022

UT Team

Kristen Phan

MSc Student in Business IT
Specialization: Enterprise Archi & IT Management + Cloud Technology

Nilay Prashant Naik

MSc Student in Business IT
Specialization: Data Science & Business

Zahra van Egdom

MSc Student in Business IT
Specialization: Enterprise Archi & IT Management

Vibha Ravindra

MSc Student in Business IT
Specialization: Data Science & Business

Sam Tran

MSc Student in Business IT
Specialization: Data Science & Business

Dovydas Ožiūnas

MSc Student in Business IT & Information Systems

Abdul Raqeeb

MSc Student in Business IT

Agenda

About BetterBe

Problem Statement

Hacker Profiling

Hackers on MITRE ATT&CK Matrix

Hackers on Network Topology

Recommendations

About BetterBe: Business Processes

BetterBe is a software company founded in 1999 that provides a customized API-based Software-as-a-Service solution called BLS to automotive leasing companies.

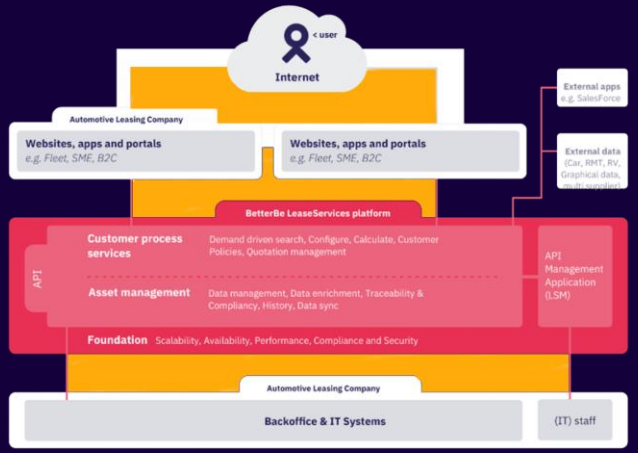
Currently serving 8 of the top 10 leasing companies in Europe

BLS allows clients to :

> Search car data real time using a vast amount of data sources

> Configure ready-to-order cars based on customer preferences

> Calculate pricing real time



Source: BetterBe's internal slide deck

About BetterBe: Stakeholder Analysis

The main business process is the BetterBe Leasing Service (BLS). The stakeholders involved are:

- BetterBe
- BetterBe clients (MeinAuto, Volkswagen, Arval…)
- Regulators (Data Protection Authorities)
- Data providers

add citations here

Research Questions & Project Methodology

research questions

Who can do

What and

How

methodology

Hacker Profiling

- Novice hackers (low motivation)
- Cyber criminals (medium)
- Corporate espionage (high)

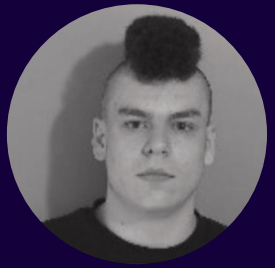
MITRE ATT&CK Framework

Attack Tree + Mock-up Network Topology

(mitigation techniques)

Warikoo,. (2014). Proposed Methodology for Cyber Criminal Profiling. Information Security Journal: A Global Perspective. 23. 10.1080/19393555.2014.931491.

Hacker Profiling: Novice (Low Motivation)



Name: Kenneth Schuchman
Age: 21

Motivation Level
Low

Skill + Resource Level
Low

Attack Severity
Low - Medium

Pleaded guilty as a creator and operator of multiple DDoS IoT botnets, including Satori.

Motives:

- Go after attention + money, not necessarily after BetterBe
- Want to prove their abilities and gain respect in the hacking community

Personality Traits:

- Brash + greedy

Hackers in Action:

MITRE Attack Category	MITRE Attack Technique	Attack Tools	Impact on BB	Impact on BB Clients	Impact on Lessees
Impact	Network denial of service	Botnets	X	X	
Resource development	Acquire Infrastructure: Botnet	Stress testers	X	X	
Impact	Endpoint denial of service	Botnets	X	X	
Reconnaissance	Active scanning	Security scanners e.g. Zenmap to find open ports	X		
Collection	Adversary-in-the-middle	Packet sniffers e.g. Wireshark	X		

Hacker Profiling: Cyber Criminals (Medium Motivation)

Name: Adrian Lamo
Age: Deceased

Motivation Level
Medium - High

Skill + Resource Level
Medium

Attack Severity
Medium - High

I believe in a world where all these things can happen, even if I have to do them myself

Motives:

- Target SMEs with limit resources yet high-profile clientele for financial gain + intellectual property (e.g. source code)

Personality Traits:

- Moderately skilled + highly motivated

Hackers in Action:

MITRE Attack Category	MITRE Attack Technique	Attack Tools	Impact on BB	Impact on BB Clients	Impact on Lessees
Credential Access	Credential Stuffing	Sentry MBA, Account Hitman, Vertex and Apex.	X	X	
Initial Access	Exploit Public-Facing Application; Trusted Relationship; External Remote Services:	SQL injection tools (e.g. SQL map, Jsql INjection, BBQSQL, DSSS, EXPLO, BLISQY)	X	X	
Persistence; Privilege Escalation	SSH Authorised Keys; Access Token Manipulation	Mimikatz and Windows credential editor	X		
Impact	Data Encrypted for Impact (Ransomware) Endpoint Denial of Service	Solarwinds sem tool, HULK, LOIC, Xoic, Slowloris	X	X	

Hacker Profiling: Corporate Espionage (High Motivation)

Name: Michael Calce
Age: 38

Motivation Level: High

Skill + Resource Level: High

Attack Severity: Medium - High

In the hacking world, security is more of a response than a proactive measure. They wait for hackers to attack and then they patch, based on the attacks.

Motives:

- Hires cyber crime syndicates to target BetterBe for financial gain + reputation damage e.g. a leasing company wants to tamper with the pricing calculation for its competitor

Personality Traits:

- Highly skilled + motivated

Hackers in Action:

MITRE Attack Category	MITRE Attack Technique	Attack Tools	Impact on BB	Impact on BB Clients	Impact on Lessees
Initial access & Lateral movement	Phishing & remote service session hijacking	Advanced Peristent Threat,APT, in combination with spear-phishing for BYOD	X	X	X
Impact	Endpoint & network denial of service	Generator of slow Denial-of Service attacks (e.g. Slowloris)	X	X	

https://bit.ly/3rrhicb, https://bit.ly/3nwbSvh, https://bit.ly/3KgUXGP, https://bit.ly/34Lqy9Y

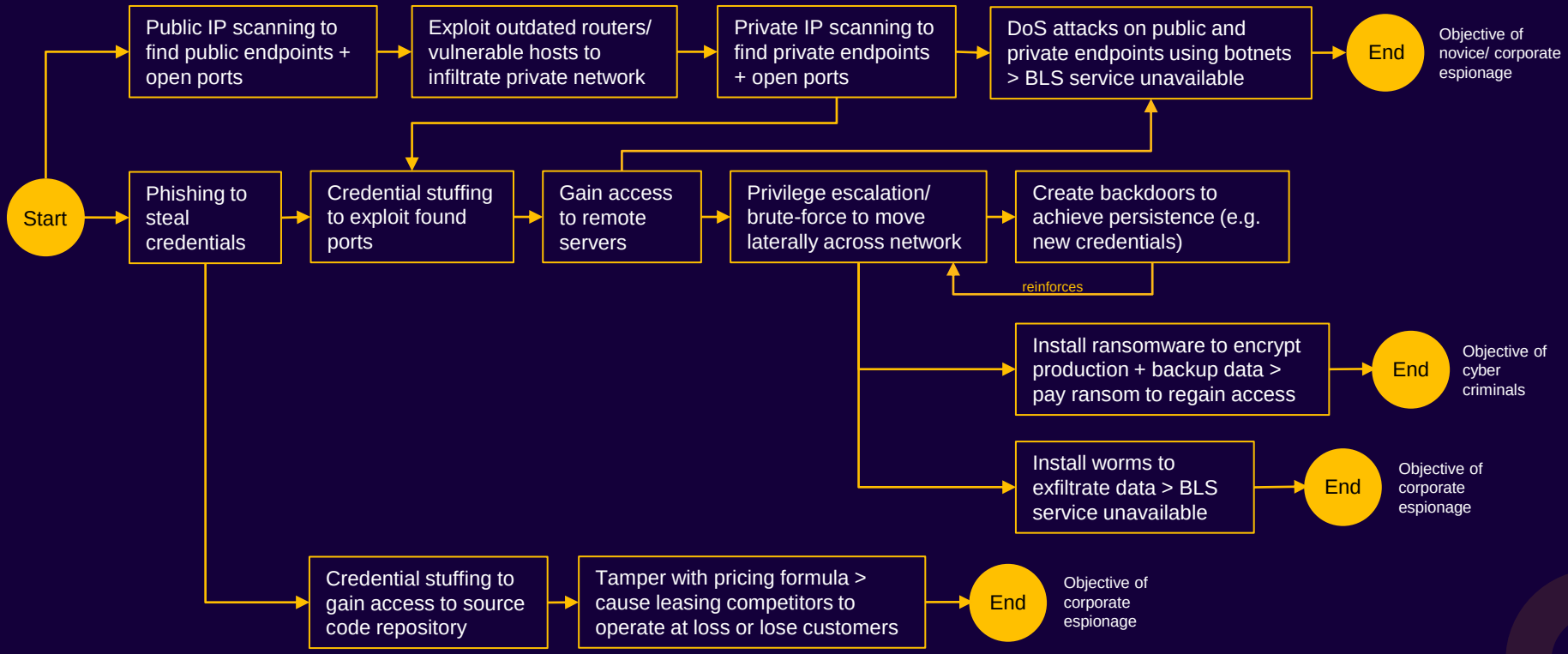
Hackers on MITRE ATT&CK Matrix

Recon-naissance	Resource Development	Initial Access	Persistence	Privilege Escalation	Credential Access	Lateral Movement	Collection	Impact
Active scanning	Acquire infra-structure	Phishing	SSH authorized keys	Access token manipulation	Credential stuffing	Remote service session hijacking	Adversary-in-the-middle	Endpoint denial-of-service
		Exploit public-facing application						Network denial-of-service
		Trusted relations						
		External remote services						

- MITRE attack technique deployed by novice
- MITRE attack technique deployed by cyber criminals
- MITRE attack technique deployed by cyber crime syndicates
- MITRE attack technique deployed by more than one hacker types

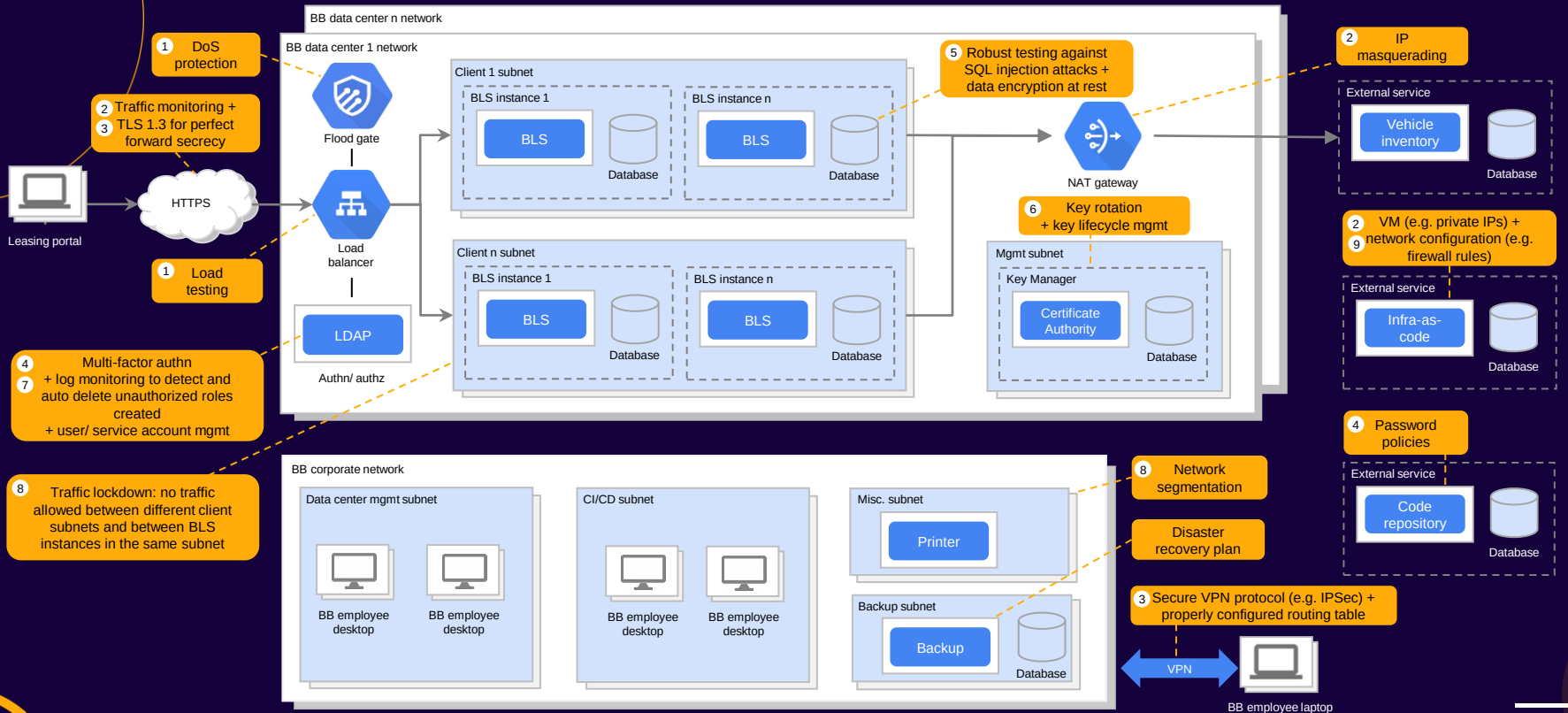
https://attack.mitre.org/tactics/enterprise/

Hackers on Attack Tree



* T-Mobile hack involved exposed router

Network Topology: Mitigation Techniques



Mitigation technique
MITRE attack technique

1 DOS attack
2 Active scanning
3 Adversary-in-the-middle
4 Credential stuffing
5 Exploit public-facing App
6 SSH authorized keys
7 Trusted relationships
8 Remote service session hijacking
9 Acquire infrastructure

https://attack.mitre.org/tactics/enterprise/

Recommendations

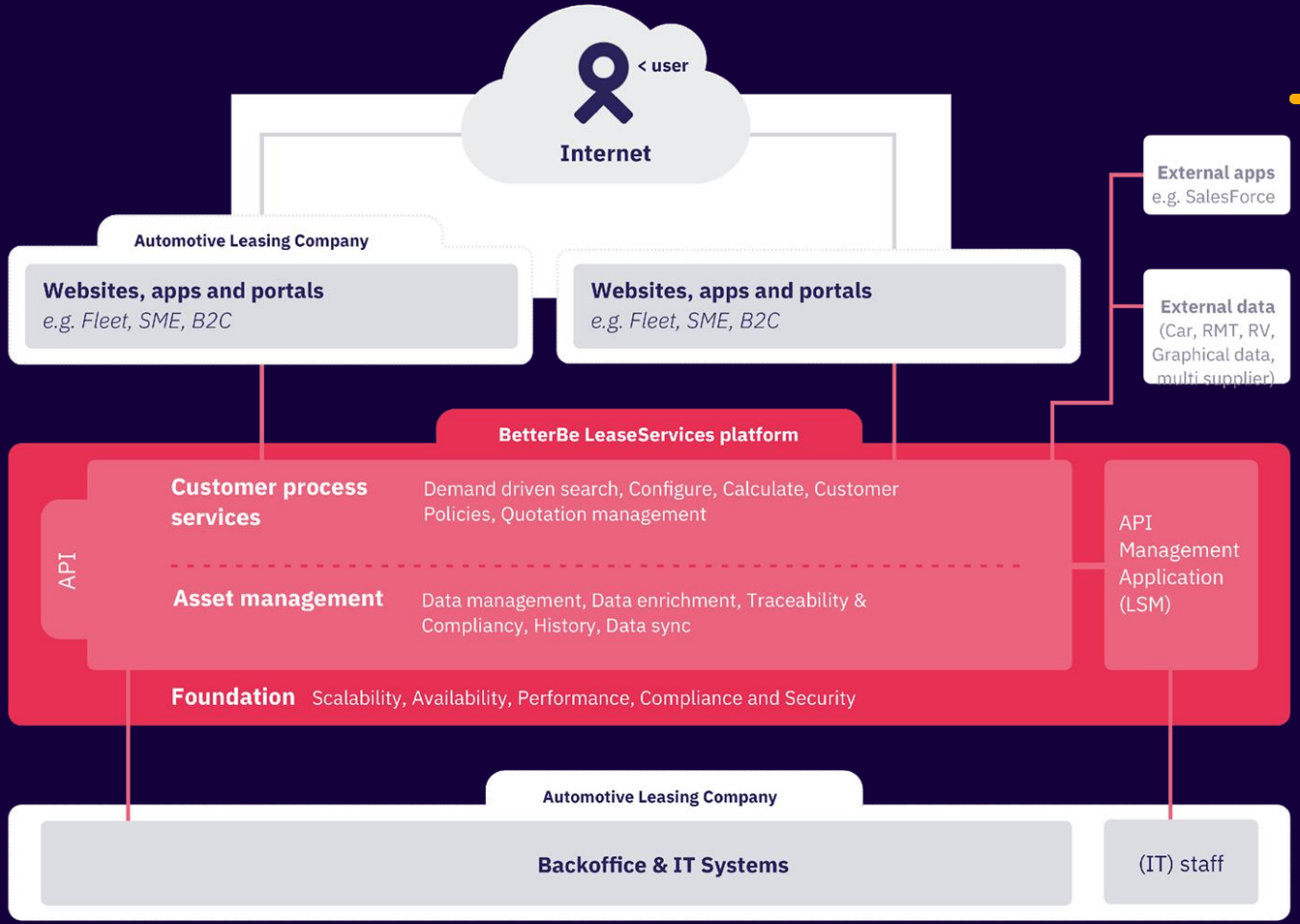
Cybersecurity Is a Journey, Not a Destination

Hacker Profiling
Validate the proposed hacker profiles (‘who’) and hacking techniques (‘what’)

Attack Tree + Network Topology
Validate attack tree + proposed mitigation techniques to safeguard against identified hacking techniques (‘how’)

Implementation
Prioritize and implement best practices based on cost-benefit analysis

Monitoring
Monitor new threats and emerging security technologies


< user
Internet
External apps
e.g. SalesForce
External data
(Car, RMT, RV, Graphical data, multi supplier)
Automotive Leasing Company
Websites, apps and portals
e.g. Fleet, SME, B2C
Websites, apps and portals
e.g. Fleet, SME, B2C
BetterBe LeaseServices platform
API
Customer process services
Demand driven search, Configure, Calculate, Customer Policies, Quotation management
Asset management
Data management, Data enrichment, Traceability & Compliancy, History, Data sync
API Management Application (LSM)
Foundation
Scalability, Availability, Performance, Compliance and Security
Automotive Leasing Company
Backoffice & IT Systems
(IT) staff