UPPSALA UNIVERSITET CAMPUS GOTLAND
Institutionen för informatik och media
Utbildningsprogram: Kandidatprogram i Systemvetenskap (inriktning Programvaruteknik)
Kursansvarig lärare: Millan Lundgren

Datum: [7/12/22]

Rapport om Hotmodellering

IT-säkerhet, 7,5 hp

Adam El Soudi

1 Problemformulering

PillMedTech vill utveckla deras applikation så att det går att registrera sjukfrånvaro. Anställda ska därför kunna logga in hemifrån för att göra en sjukanmälan eller anmälan av vård av sjukt barn, samt kunna logga ut. Pågrund av detta kommer känslig data kring personuppgifter att behöva överföras och kräver därför att applikationen utvecklas med säkerhet i åtanke.

1.1 Antaganden

- Det finns en klar databas som han hantera uppgifterna om de anställda (namn, personnummer, anställningsnummer, adress, telefon, mail, sina barns namn).

- Anställda har giltiga inloggningsuppgifter.

- Anställda har tillgång till rätt sidor beroende på deras roll.

2 Resultat

Den här rapporten går igenom hur PillMedTech ska gå vidare för att uppnå funktionerna som ska tilläggas till applikationen med säkerhet i fokus.

2.1 Kravhantering

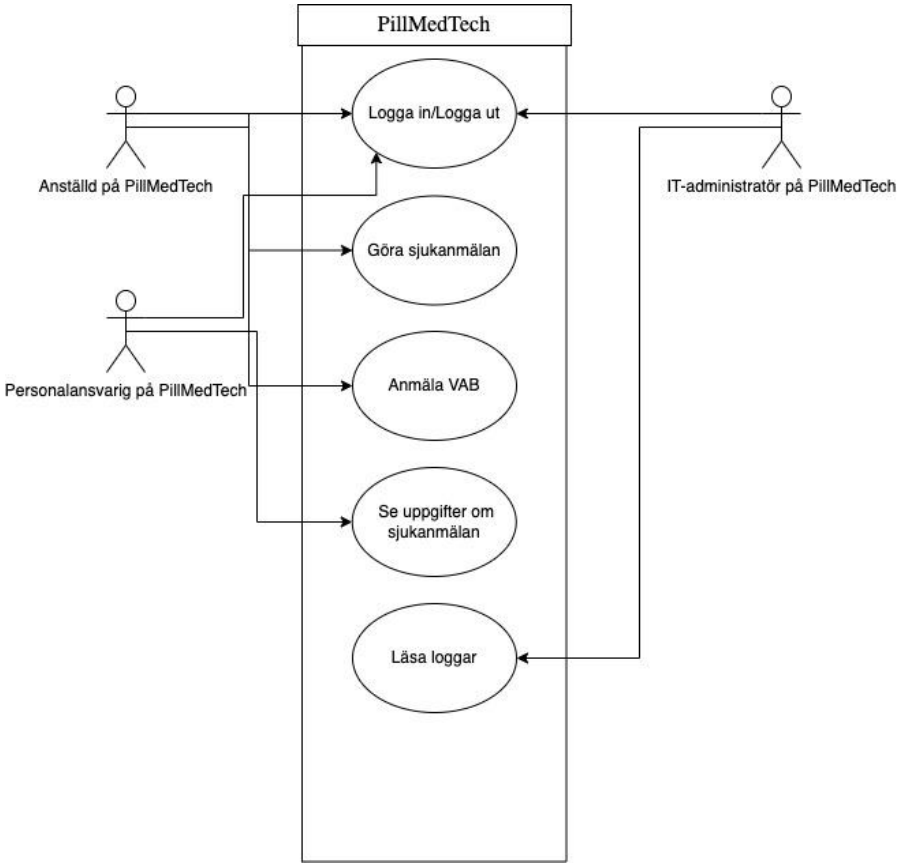
Applikationen som ska byggas är en webbsajt för att hantera sjukskrivningar och de användningsfall som identifierats ser vi i diagrammet nedan. Beskrivning av varje fall finns i bilaga 1.

De aktörer som vi ser som kommer att använda systemet är:

Anställda på PillMedTech ska ha inlogginings uppgifter (användarnamn och lösenord). Dem ska kunna logga in och logga ut. Det ska vara möjligt att göra en sjukanmälning och/eller fylla i VAB-informationen.

Personalansvarig på PillMedTech ska ha inloggnings uppgifter (användarnamn och lösenord). Hen ska kunna logga in och logga ut. Hen kan fylla i anställningsnummer för den person vars anmälan hen vill se och systemet ska itur logga händelsen.

IT-administratören på PillMedTech ska kunna öppna upp och visas alla loggarna i systemet.



2.2 Externa beroenden

.Net Core MVC är skapat av Microsoft så man kan lita på att det kommer att vara väldigt säkert att använda. Windows Server 2022 är också säkrare än vad det var tidigare. En av anledningarna till detta är att Windows Server 2022 encriptar innan datalagringen skett. Detta leder även till bättre prestanda än tidigare Windows Server versioner[1].

Med tanke på att en databas kommer att vara en stor del av applikationen kan det bli lite jobbigt att använda .NET Core MVC. Beroende på vilket operativsystem man jobbar på är koden som krävs för att arbeta med databasen annorlunda. För dem som jobbar med OS (Apple datorer) måste dem ladda hem ett program som heter Docker som gör det möjligt att koppla koden till en databas. Detta är inte

[1] Posey, Brien. "Windows Server 2022 Security Hardening Guide for Admins." SearchWindowsServer, 26 Apr. 2022.

nödvändigtvis ett problem men kan kräva lite extra arbete i börjar för att se till att allting funkar som det ska efteråt.

Eftersom en stor del av utvecklandet av applikationen handlar om att logga in är .NET Core MVC ett bra val då det är enkelt att skapa roller och inloggningar åt anställda samt att det blir säkrare eftersom att den datan med inloggningar inte finns tillgänglig via websidan man loggar in på eller den man kommer till när man är inloggad.

ID	Beskrivning
1	Webbsajten för sjukskrivning kommer att köras på Windows server 2022 som är placerad på PillMedTech.
2	Systemet kommer att byggas i .NET Core MVC (.NET 6) med språket C#
3	Databasen kommer att finns på en SQL server 2022 även den placerad på PillMedTech
4	Uppkopplingen till webbserver går över offentliga nätverk medan kopplingen till databasen går över ett privat nätverk
5	Webbservern befinner sig bakom en brandvägg och kommunikationen med den är endast tillgänglig över TLS

2.3 Ingångspunkter

ID	Namn	Beskrivning
1	HTTPS Port	Inloggnings vyn kan alla nå men sen finns det en specifik vy som användaren kommer till beroende på deras roll när de loggar in.
1.1	PillMedTech huvudsida	Detta är första sidan som användaren möts med när dem går in på PillMedTech's websida.
1.2	Login sida	Anställda, Personansvarig och IT-administratör på PillMedTech måste logga in för att komma åt user-cases.

1.2.1	Login Funktion	Login funktionen kollar så att den inmatade inloggningen gjord av användaren och jämför det med inloggnings datan i databasen för att se om det stämmer eller inte.
1.3	Search Entry Page	Den här sidan används för att skriva in en sök query.

2.4 Tillgångar

		Konfidentialitet	Riktighet	Tillgänglighet
3	Allvarlig Hög skyddsnivå	**K3** Information där förlust av konfidentialitet innebär **allvarlig** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	**R3** Information där förlust av riktighet innebär allvarlig **negativ** påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	**T3** Information där förlust av tillgänglighet innebär **allvarlig** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.
2	Betydande Utökad skyddsnivå	**K2** Information där förlust av konfidentialitet innebär **betydande** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	**R2** Information där förlust av riktighet innebär **betydande** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	**T2** Information där förlust av tillgänglighet innebär **betydande** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.
1	Måttlig Grundläggande skyddsnivå	**K1** Information där förlust av konfidentialitet innebär **måttlig** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	**R1** Information där förlust av riktighet innebär **måttlig** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	**T1** Information där förlust av tillgänglighet innebär **måttlig** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.
0	Ingen Ingen skyddsnivå	**K0** Information där förlust av konfidentialitet **inte medför någon** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	**R0** Information där förlust av riktighet **inte medför någon** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	**T0** Information där förlust av tillgänglighet **inte medför någon** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.

För att anställda ska kunna logga in och kunna ansöka om sjukfrånvaro eller vård av barn måste systemet kunna hämta och spara ner känslig data. En personaldatabas krävs för att detta ska kunna gå och där kommer känslig data av anställda behöva sparas ner som namn, personnummer, anställningsnummer, adress, telefon, mail, sina barns namn. Konsekvensnivån på dessa är olika när det kommer till hur viktigt det är att säkra dem.

	Konfidentialitet	Riktigthet	Tillgänglighet
Personuppgifter	K2	R3	T2
Inlogginingsuppgifter	K3	R3	T3
Barnens personuppgifter	K3	R2	T2

Personuppgifter:
Jag har gett konfidentialitet K2 då det är väldigt viktigt att personuppgifterna inte kommer ut. Men det ger inte jätte stora svårigheter för verksamheten ska nå sitt mål. För riktighet har jag gett en R3 då det är viktigt att personuppgifterna är korrekta i systemet för att rätt information matchar rätt person. Detta är också viktigt att följa då GDPR måste följas[2] och bör krypteras. Tillgängligheten har jag gett T2 då det igen är viktigt att systemet vet vem som är vem och personuppgifterna är ett bra sätt att identifiera dem anställda.

Inloggningsuppgifter:
För inloggningsuppgifter har jag gett konfindentialiteten K3 då det kan ställa till det om dem inte är säkrade. Jag har också gett riktighet R3 samt Tillgänglighet T3. När det kommer till inloggningsuppgifterna ska det vara så säkert som det går annars finns risken att någon få tag på dem som inte ska kunna komma in på systemet och sabortera. Därför ska inloggningsuppgifterna vara krypterade[3].

Barnens personuppgifter:
Barnens uppgifter har jag gett betygen/klassningarna ovan. Barnens personuppgifter ska ingen kunna komma åt så det är viktigt att dem är skyddade. Det är känslig data och anställda ska kunna förlita sig på att den datan är väl skyddad och kanske även kryperad.

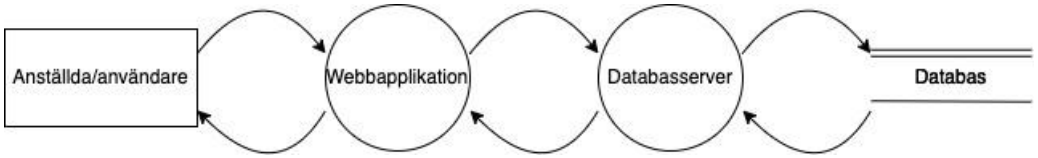
2.5 Förtroendenivåer

ID	Namn	Beskrivning
1	Anonym användare	En användare som är på PillMedTech's sida men som inte har en giltig inlogging / ett konto.
2	Användare med giltig inloggning	En användare som är anställd på PillMedTech och har en giltig inlogging / ett konto.
3	Användare med ogiltig inloggning	En användare som försöker logga in på hemsidan med ogiltiga inloggningsuppgifter

[2] Koch, Richie. "What Is Considered Personal Data under the EU GDPR? - GDPR.eu." GDPR.eu, 13 Feb. 2019.
[3] Carklin, Nicolette. "The Ability to Secure Data for Remote Access." Parallels Remote Application Server Blog - Application Virtualization, Mobility and VDI, 15 June 2022.

4	Personansvarig på PillMedTech	Personansvarig på PillMedTech kan fylla i anställningsnummer för den person vars anmälan dem vill se.
5	IT-administratör på PillMedTech	IT-administratör på PillMedTech kan se och läsa loggarna över alla viktiga händelser i systemet.

2.6 Dataflödesdiagram



Dataflödesdiagramet visar processen och hur systemet kommunuserar med dem olika komonenterna som används. Användaren i detta fall är dem anställda som ska kunna logga in på webbapplikationen. Webbapplikationen ska i sin tur gå vidare till databasservern som går vidare till själva databasen och hämtar den rätta datan (namn, personnummer, anställningsnummer, adress, telefon, mail, sina barns namn) om den anställda. Detta skickas sen tillbaka genom samma system till användaren som nu har kommit till rätt sida/vy som hen har tillgång till. Där kan dem nu göra sin ansökan via webbapplikationen som sen går igenom samma steg och lägger till den nya datan i databasen som personalansvarig på PillMedTech kan se. Personansvarig går igenom samma process när hen också loggar in fast dem kommer till en annan vy som dem har tillgång till.

2.7 Hot mot systemet och dess motåtgärder

Det finns 3 olika potentiella hot som jag har identifierat, spoofing, tampering och elevation of privilege. Här kommer jag att förklara vad dessa uttryck betyder och vad som bör implementeras för att minska risken eller konsekvenserna av dem.

Spoofing är ett hot som innehbär att attackeraren försöker få åtkomst till en användares (i det här fallet en anställd hos PillMedTech) användarnamn och lösenord. Enligt Alwarebytes är spoofing: “[...]when

someone or something pretends to be something else in an attempt to gain our confidence, get access to our systems, steal data, steal money, or spread malware"[4]. För att minska risken och konsekvenserna för spoofing är det viktigt att dem anställda har ett starkt lösenord genom att följa lösenordspolicyn som finns längre ner i rapporten. Detta kommer att minska risken att attackeraren ens får tillgång till kontot och vyn. Enligt artikeln *What Is Spoofing and How Can You Prevent it?* skriven av Ivan Belcic & Ellie Farrier; "If a spoofer manages to obtain your login credentials, they won't be able to do much if you already have a new password. I syfte att minska konsekvenserna bör anställda regelbundet ändra deras lösenord då detta gör attackeraren inte kan komma åt kontot eller vyn om dem redan har inloggningsuppgifterna[5].

Det andra hotet som finns kallas för tampering. Tampering är ett hot med målet att ändra på data, i databasen i detta fall. För att minska risken till att det här sker ska databasen vara svår att nå. Man vill inte att attackeraren ska kunna komma åt databasen via hemsidan till exempel och därför är det också bra att programmet byggs upp med hjälp av .NET core MVC. Det tillåter oss att ha dem separerade och låta programmet sköta kopplingen mellan dem olika delarna av systemet med hjälp av controllers. Kryptering av data är också et åtgärd som kommer att minska konsekvensern av en tampering attack. Som exempel kan man kryptera känslig information som är sparad i databasen. Det gör så att om attackeraren skulle komma åt databasen, kommer den känsliga informationen synas i ett krypterat format som inte går att använda utan en nyckel[6].

Elevation of privilege betyder i princip att få obehörig tillgång till privilegierade konton där man kan få tag på information eller sabotera ett system. I det här fallet skulle en attackerare kunna försöka att komma åt inloggninguppgifterna av IT-administratören och på så sätt komma åt

[4] "Spoofing | What Is a Spoofing Attack? | Spoofing Detection & Prevention." Malwarebytes, www.malwarebytes.com/spoofing. Accessed 7 Dec. 2022.

[5] Belcic, Ivan, and Ellie Farrier. "What Is Spoofing and How Can I Defend against It?" What Is Spoofing and How Can I Defend against It?, 3 June 2021, www.avast.com/c-spoofing. Accessed 7 Dec. 2022.

[6] Cypress Data Defense. "How to Prevent Data Tampering in Your Business." Www.cypressdatadefense.com, 24 June 2020, www.cypressdatadefense.com/blog/data-tampering-prevention/. Accessed 7 Dec. 2022.

loggarna. Loggarna innehåller ip-adresser som kan vara känslig data om man kan identifiera vem personen är via den[7]. För att minska risken för att något sånt här händer är det viktigt att alla privilegierade konton är så säkrade som möjligt[8]. Om man ska satsa extra pengar på säkerheten och krypteringen är det här man ska börja. Det är viktigt att förstå att när vi krypterar är det nyckeln vi vill skydda, det är den som används för att se den riktiga datan.

2.8 Lösenordspolicy

- Lösenordet ska vara minst 10 tecken
- Lösenordet ska ha minst ett tecken
- Lösenordet ska ha minst en stor bokstav
- Lösenordet ska ha minst en liten bokstav
- Lösenordet ska ha minst ett nummer
- Ett lösenord går inte att skapa om det inte möter alla dem övre kriterierna.

[7] Aleksandrova, Maya. "Does the IP Address Represent Personal Data?" Cms.law, cms.law/en/bgr/publication/does-the-ip-address-represent-personal-data. Accessed 7 Dec. 2022.

[8] PREVIEW:
Kingatua, Amos. "Privilege Escalation Attacks, Prevention Techniques and Tools." Geekflare, 17 Nov. 2020, geekflare.com/privilege-escalation-attacks/. Accessed 7 Dec. 2022.

3 Sammanfattning

Den här rapporten har gått igenom och förklarat kravhantering, externa beroenden, ingångspunkter, tillgångar, förtroendenivåer och hot mot systemet på PillMedTech samt skapat en lösenordspolicy. Alla dessa rubriker kommer att hjälpa PillMedTech att skapa nya funktionaliteter angående inloggning, roller och konton på ett säkert sätt. Det kommer också minska risken för att en attack mot systemet, vare sig det är mot databasen eller websidan, sker. Det är viktigt att komma ihåg att alltid tänka att någon vill attackera systemet och att konstant försöka att förstärka säkerheten för att driva bort dem. Om det är svårare för attackeraren att bryta sig in kommer dem förmodligen gå vidare någon annanstans.

4 Referenslista

- Posey, Brien. “Windows Server 2022 Security Hardening Guide for Admins.” SearchWindowsServer, 26 Apr. 2022, www.techtarget.com/searchwindowsserver/tip/Windows-Server-security-hardening-guide-for-admins#:~:text=Windows%20Server%202022%20performs%20encryption. Accessed 1 Dec. 2022.

- Koch, Richie. “What Is Considered Personal Data under the EU GDPR? - GDPR.eu.” GDPR.eu, 13 Feb. 2019, gdpr.eu/eu-gdpr-personal-data/. Accessed 6 Dec. 2022.

- Carklin, Nicolette. “The Ability to Secure Data for Remote Access.” Parallels Remote Application Server Blog - Application Virtualization, Mobility and VDI, 15 June 2022, www.parallels.com/blogs/ras/the-ability-to-secure-data-for-remote-access/#:~:text=The%20primary%20goal%20of%20encrypting. Accessed 6 Dec. 2022.

- Conklin, Larry. “Threat Modeling Process | OWASP.” Owasp.org, owasp.org/www-community/Threat_Modeling_Process. Accessed 6 Dec. 2022.

- “Spoofing | What Is a Spoofing Attack? | Spoofing Detection & Prevention.” Malwarebytes, www.malwarebytes.com/spoofing. Accessed 7 Dec. 2022.

- Belcic, Ivan, and Ellie Farrier. “What Is Spoofing and How Can I Defend against It?” What Is Spoofing and How Can I Defend

against It?, 3 June 2021, www.avast.com/c-spoofing. Accessed 7 Dec. 2022.

- Aleksandrova, Maya. "Does the IP Address Represent Personal Data?" Cms.law, cms.law/en/bgr/publication/does-the-ip-address-represent-personal-data. Accessed 7 Dec. 2022.

5 Bilagor

5.1 Detaljerad beskrivning av användningsfall

Logga in

Användningsfall	1. Logga in
Primär aktör:	Anställd på PillMedTech
Förutsättningar:	Användaren har hemsidan öppen framför sig
Grundflöde:	1. Användaren väljer att logga in 2. Systemet visar inloggningssidan 3. Användaren fyller i användarnamn och lösenord 4. Systemet kontrollerar uppgifterna 5. Systemet visar korrekt startsida beroende på behörighet 6. Systemet loggar händelsen
Undantagsfall:	4. Uppgifterna är inte korrekta 1. Systemet ger generellt felmeddelande om att inloggningen inte fungerade 2. Systemet loggar händelsen

Göra sjukanmälan

Användningsfall	2. Göra sjukanmälan
Primär aktör:	Anställd på PillMedTech
Förutsättningar:	Användaren är inloggad (se fall #1)
Grundflöde:	1. Användaren fyller i sjukanmälan 2. Användaren väljer att spara anmälan 3. Systemet validerar information 4. Systemet sparar informationen 5. Systemet visar tacksida som bekräftar att anmälan är mottagen 6. Systemet loggar händelsen
Alternativt flöde:	1. Användaren väljer att göra sjukanmälan med läkarintyg 1. Användaren markerar att läkarintyg finns 2. Tillbaka till grundflöde steg 2

Anmäla VAB

Användningsfall	3. Anmäla VAB
Primär aktör:	Anställd på PillMedTech
Förutsättningar:	Användaren är inloggad (se fall #1)
Grundflöde:	1. Användaren fyller i VAB-informationen 2. Användaren väljer att spara anmälan 3. Systemet validerar information 4. Systemet sparar informationen 5. Systemet visar tacksida som bekräftar att anmälan är mottagen 6. Systemet loggar händelsen

Se uppgifter om sjukanmälningar/VAB

Användningsfall	4. Se uppgifter om sjukanmälan
Primär aktör:	Personalansvarig på PillMedTech
Förutsättningar:	Användaren är inloggad (se fall #1)
Grundflöde:	1. Användaren fyller i anställningsnummer på den person vars anmälan man vill se 2. Systemet visar en tabell med uppgifter om VAB och/eller sjukanmälningar 3. Systemet loggar händelsen
Undantagsfall:	2. Det finns inga sjukanmälningar/VAB 1. Systemet ger ett meddelande om att inga sjukanmälningar fanns 2. Systemet loggar händelsen

Läsa loggar

Användningsfall	5. Läsa loggar
Primär aktör:	IT-administratör på PillMedTech
Förutsättningar:	Loggar innehåller tid, användare, ip-adress och åtgärd (händelse).
Grundflöde:	1. Administratören loggar in 2. Administratören öppnar upp loggarna 3. Systemet visar alla loggar

	4. Administratören kan se och läsa loggarna
Undantagsfall:	1. Administratören loggar in 2. Administratören öppnar upp loggarna 3. Det finns inga loggar 4. Administratören loggar ut