|  |
| --- |
| Rapport |

IoT inom sjukvården

*Säkerhetsrisker och eventuella lösningar*

|  |
| --- |
| *Författare:* Emil Ulvagården  *Termin:* Ht 23  *Kursnamn:* Teknisk kommunikation  *Kurskod:* 1ZT010 |



Sammandrag

Syftet med rapporten är att undersöka de risker som finns med att koppla upp IoT på internet samt hur sjukvårdsenheter kan påverkas av eventuella angripare. Rapporten ska även undersöka vilka eventuella lösningar som kan motverka säkerhetsriskerna med uppkopplad IoT. Rapporten är en litteraturstudie och de flesta källor är vetenskapligt granskade artiklar. Två säkerhetsrisker som nämns i rapporten är *distributed denial of service* (DDOS) och *medjacking.* De tre säkerhetslösningar som tas upp i rapporten för att motverka säkerhetsriskerna är användning av reservsystem, tre olika behörighetsmetoder samt användning av *honeypots*. Det är viktigt att känna till att det finns fler säkerhetsrisker och säkerhetslösningar än de som tas upp i rapporten. Säkerhetsriskerna och säkerhetslösningarna är inte specifika för IoT utan de förekommer för alla uppkopplade system.

The reason for the rapport is to investigate the risks associated with connecting IoT to the internet and how these medical devices can be affected by possible attackers. The report will also examine what possible solutions can counteract the security risks of connected IoT. The report is a literature review and most of the sources are peer reviewed articles. Two vulnerabilities mentioned in the report are distributed denial of service (DDOS) and medjacking. The three security solutions discussed in the report to mitigate the security risks are the use of backup systems, three different authentication methods and the use of honeypots. It is important to know that there are more security risks and solutions than those mentioned in the report. The security risks and solutions are not specific for IoT, but they exist for all connected systems.

Nyckelord

IoT, Sjukvård, Säkerhetsrisker, Säkerhetslösningar

Innehåll

1 Inledning I

1.1 Syfte och frågeställningar I

1.2 Metod och material I

2 Resultat II

2.1 Säkerhetsrisker II

2.2 Säkerhetslösningar II

3 Diskussion och slutsatser IV

3.1 Diskussion IV

3.2 Slutsatser IV

Referenser V

# Inledning

*Internet of Things* (IoT) används mer och mer i sjukvården. Uppkoppling av dessa enheter medför förbättringar för både patienter och personal [1]. Uppkopplade enheter tillåter sjukhuset att spara och analysera patientdata över längre tid. Detta gör att flera patienter kan övervakas från en dator. IoT är mikrochips som ofta kopplas till sensorer, vars uppgift är att samla och byta data med varandra. IoT i sjukvården omfattar alla sensorer som används för att bevaka en patients fysiska tillstånd. Det kan vara utrustning som till exempel en sensor för elektrokardiografi (EKG) eller en insulinpump.

Problem uppstår när IoT kopplas upp på internet på grund av säkerhetsrisker. År 2015 hittades över 60 000 medicinska system exponerade på internet. Dessa var uppkopplade via ett gammalt operativsystem (OS) med flera kända säkerhetsproblem. Under granskningen av dessa medicinska enheter framkom det att icke behöriga varit uppkopplade tiotusentals gånger [1].

Enligt säkerhetsforskare hos Huntress är flera hälso- och sjukvårdsorganisationer i USA mål för hackare [2]. Forskarna upptäckte hackarna på två sjukvårdsorganisationer och dess aktiviteter tyder på förberedelse till en potentiell attack. De observerades den 28 oktober 2023 och hackarna är troligtvis fortfarande aktiva och har tagit flera steg för att garantera åtkomst till systemet, så som att installera programmet ScreenConnect. ScreenConnect används för att överföra filer från sjukvårdsorganisationerna. ScreenConnect har spårats till en domän som används av *Transaction Data systems* (TDS), ett ledningssystem för apotek som används i alla 50 delstater.

## Syfte och frågeställningar

Syftet med rapporten är att undersöka de risker som uppstår vid uppkoppling av IoT på internet samt hur enheter kan påverkas av eventuella angripare. Rapporten ska även undersöka vilka eventuella lösningar som kan minska säkerhetsriskerna med uppkopplad IoT. De frågor som rapporten ska undersöka är:

RQ1: Vilka säkerhetsrisker finns för uppkopplade sjukvårdsenheter?

RQ2: Hur kan säkerhet garanteras för uppkopplade sjukvårdsenheter?

## Metod och material

Denna rapport är en litteraturstudie. Majoriteten av källorna i rapporten är vetenskapligt granskade artiklar tagna från OneSearch och en tidningsartikel. För att minimera risken för ekonomiskt beroende källor har informationen kontrollerats så att inga andra företag nämns i texterna. På så vis minskas risken för att en källa vill sprida något negativt om ett annat företag. En av källorna tar dock upp ett annat företag för att på så vis specificera vilken enhet som påverkats och hur.

# Resultat

I den första delen av detta kapitel redovisas några av de säkerhetsrisker som kan uppstå inom vården när IoT kopplas upp på internet. I den andra delen redovisas några av metoderna för att förbättra säkerheten hos uppkopplade sjukvårdsenheter.

## Säkerhetsrisker

Säkerhetsrisker för uppkopplade IoT-lösningar inom sjukvården består av olika typer av cyberattacker [1], [3]. En av dessa attacker är *distributed denial of service* (DDOS), en attack där kommunikation mellan enheter helt eller delvis bryts när den ena enheten överbelastas. En annan typ av cyberattack mot sjukvårdsenheter är *medjacking*, en form av attack där obehöriga tar kontroll över medicinsk IoT för att antingen ändra doseringar eller funktioner. Vanligast är att dessa enheter kapas för att angripare med hjälp av dem ska få tillgång till mer centrala system som databaser med mer kritisk information.

År 2008 släpptes en insulinpump där patienter kunde reglera mängden insulin med en trådlös kontroll [1]. Denna enhet visade sig sakna kryptering mellan kontrollen och pumpen, vilket tillät obehöriga reglera mängden insulin patienten tog emot. År 2015 kom en rapport om att olika medicinska enheter var infekterade med virus som skickade information som lösenord och patientinformation till obehöriga [1]. Dessa enheter gav även i vissa fall obehöriga tillgång till sjukhusets nätverk samt interna system.

## Säkerhetslösningar

För att garantera att säkerheten inte fallerar delas säkerhetsåtgärderna in i två olika grupper, icke tekniska och tekniska åtgärder [3]. Förbättring av de icke-tekniska lösningarna görs genom att man utbildar personal till att bli mer svårlurade och säkerhetstänkande. Förbättringar av de tekniska åtgärderna görs genom att införa olika säkerhetslösningar. Några av dessa lösningar är bättre behörighetsmetoder, reservsystem och *Honeypots*.

De olika behörighetsmetoderna är *singlefactor authentication* (SFA), *twofactor authentication* (TFA) och *multifactor authentication* (MFA). Den behörighetsmetod som är säkrast är MFA följt av TFA och slutligen SFA. Vid användning av SFA krävs endast ett användarnamn och ett lösenord för att fastställa att rätt användare har tillgång till enheten. Vid användning av TFA används utöver SFA ytterligare någon säkerhetsåtgärd för att fastställa användarens identitet. Med MFA utvecklas TFA ytterligare ett eller flera steg med hjälp av tredjepartstjänster eller skanning av specifika fysiska kroppsdelar som iris eller näthinnan. Dessa metoder används för att säkerställa att endast behörig personal kommer åt känslig information [3].

För att minimera den påverkan som en DDOS-attack kan medföra på livsviktig IoT krävs vissa säkerhetsåtgärder, t.ex. användning av reservsystem. Det krävs reservsystem som kan aktiveras snabbt ifall en uppkoppling inte kan upprätthållas. Enheternas data ska alltid kunna nå behörig och aktuell personal. Detta sker genom att ha en eller flera reservservrar redo att ta emot information ifall huvudservern misslyckas. Det krävs även att IoT-enheterna har en form av reservenhet som kan skicka och ta emot information ifall huvudenheten misslyckas [3].

Honeypots utger sig för att vara riktiga system, men de är egentligen en fälla för obehöriga individer. De kan upptäcka obehöriga användare på ett system och se vilka tillvägagångssätt och verktyg som används. Med hjälp av en honeypot kan säkerheten hos IoT uppdateras med aktuella metoder i åtanke. De kan även användas för att studera hur IoT attackeras samt vilken information som obehöriga kan komma åt.

För att IoT säkert ska kunna skicka känslig information över internet kan användning av *blockchains* (blockkedja) tillkomma i framtiden [4]. En blockkedja är en distribuerad huvudbok med växande listor över block som är säkert sammanlänkade via kryptografiska hashar. Blockkedjor används för datainsamling, lagring och distribution. Alla datatransaktioner är automatiskt validerade och verifierade. Det garanterar datasäkerhet och integritet. Kryptografiska hashar tillåter skapandet av unika identifieringskoder för olika block. De skapar även spårningsfunktioner till föregående blocks hash. En kryptografisk hashfunktion är en matematisk algoritm som omvandlar data till en kort kod.

# Diskussion och slutsatser

Denna rapport beskriver två säkerhetsrisker som kan förekomma med uppkopplade IoT-enheter inom sjukvården. Studien pekar på de konsekvenser som säkerhetsriskerna kan medföra samt ger förslag på några säkerhetslösningar som kan implementeras.

## Diskussion

DDOS är en typ av attack som kan medföra stora konsekvenser ifall de inte hanteras korrekt. Till skillnad från medjacking har DDOS ingenting att göra med att stjäla information från en patient eller sjukvårdsorganisationen. DDOS används för att förhindra kommunikation mellan IoT och sjukvårdsorganisationens server, vilket kan medföra försämrad datainsamling och försenad medicinsk vård. Försämrad datainsamling kan en individ överleva, men beroende på individens fysiska tillstånd kan en försenad medicinsk vård innebära dödsfall. Av dessa anledningar krävs det att IoT-enheterna alltid kan upprätthålla kontakt med sjukvårdsorganisationens servrar. De reservsystem som måste finnas tillgängliga för att undvika en DDOS-attack är alternativa servrar och användning av andra IoT-enheter. Användning av alternativa servrar medför att om huvudservern inte kan ta emot informationen kommer en annan server ta emot den så att personalen kan agera. Användning av alternativ IoT för att skicka information medför att om huvudenheten inte kan skicka data kommer en annan enhet ta över och skicka data till servern.

Medjacking handlar till skillnad från DDOS inte om att förhindra kommunikationen mellan server och IoT. Medjacking kan få lika stora om inte större konsekvenser än vad en DDOS-attack kan få. Inte bara det att en patients information kan hamna i fel händer, den information som skickas till sjukvårdsorganisationen kan vara manipulerad. Med manipulerad information är risken för felaktiga behandlingar mycket stor och risken för att andra sjukdomar inte upptäcks ökar. Medjacking kan även leda till att funktioner hos IoT ändras, vilket kan innebära ren livsfara. För att fastställa att endast behöriga individer har åtkomst till IoT bör åtminstone TFA användas, om inte MFA. I nuläget är SFA en för svag metod för att säkerställa att rätt individ har åtkomst. Honeypots bör också användas frekvent för att hålla säkerheten uppdaterad för olika enheter.

## Slutsatser

Säkerheten hos IoT är viktig och med alla hot som idag existerar krävs det att sjukvården tar ansvar, inte bara för individers fysiska hälsa utan för deras digitala säkerhet. Genom att implementera de tidigare nämnda säkerhetslösningarna minskar risken för att obehöriga ska påverka vården en individ har rätt till. Det finns fler säkerhetsrisker än de som nämnts i rapporten, och därför krävs ytterligare forskning inom området. Framtida studier kan komma att fokusera på hur implementation av blockkedjor ska används inom IoT för att säkerställa att information inte hamnar hos fel individer.

# Referenser

[1] A. Chacko och T. Hayajneh, “Security and Privacy Issues with IoT in Healthcare,” *EAI Endorsed Transactions on Pervasive Health and Technology*, vol. 4, no. 14, ss. 155079-155085, Juli 2018, DOI: [10.4108/eai.13-7-2018.155079](https://doi.org/10.4108/eai.13-7-2018.155079)

[2] B. Toulas “Hackers breach healthcare orgs via ScreeanConnect remote access.” bleepingcomputer*.* [https://www.bleepingcomputer.com/news/security/hackers-breach-healthcare-orgs-via-screenconnect-remote-access/#google\_vignette](https://www.bleepingcomputer.com/news/security/hackers-breach-healthcare-orgs-via-screenconnect-remote-access/) (2023-12-01)

[3] J. A. Yaacoub med flera, “Securing internet of medical thigs systems: Limitations, issues and recommendations,” *Future generation computer systems*, vol. 105, ss. 581-606, 2022 DOI: [10.1016/j.future.2019.12.028](https://doi.org/10.1016/j.future.2019.12.028)

[4] D. Rani med flera ,“A Secure Framework for IoT -based Healthcare Using Blockchain and IPFS,” *Security and privacy*, 2023, doi: [10.1002/spy2.348](https://doi.org/10.1002/spy2.348)