|  |
| --- |
| Rapport |

IoT inom sjukvården

*Säkerhetsrisker och eventuella lösningar*

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



Sammandrag

Syfte med rapporten är att undersöka de risker som finns med att koppla upp IoT på internet samt hur dessa enheter kan påverkas av eventuella angripare. Rapporten ska även undersöka vilka eventuella lösningar som kan motverka säkerhetsriskerna med uppkopplad IoT. Rapportens frågeställningar är:

RQ1: Vilka säkerhetsrisker finns för uppkopplade sjukvårdsenheter?

RQ2: hur kan säkerhet fastställas för uppkopplade sjukvårdsenheter?

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 behörighets metoder 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 finns för all olika uppkopplade system.

The reason for the rapport is to investigate the risks associated with connecting IoT to the internet and how these devices can be affected by possible attackers. The report will also examine what possible solutions can counteract the security risks of connected IoT. The research questions in the report are:

RQ1: What are the security risks for connected healthcare devices?

RQ2: How can security be determined for connected healthcare devices?

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 different 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 ska kopplas upp på internet, på grund av olika säkerhetsrisker. År 2015 hittades 68 000 medicinska system exponerade på internet. Dessa var uppkopplade via ett gammalt operativsystem (OS) med flertalet kända säkerhetsproblem [1]. Under undersökningen av dessa medicinska enheter framkom det att icke behöriga varit uppkopplade 55 000 gånger.

Enligt säkerhets forskare hos Huntress är flertalet hälso- och sjukvårdsorganisationer i USA mål för hackare [3]. Forskarna upptäckte hackarna på två sjukvårdsorganisationer och dess aktiviteter tyder på förberedlers till en potentiell attack. De observerades först den 28 oktober 2023 och hackarna är troligtvis fortfarande aktiva. De har tagit flertalet steg för att garantera åtkomst till systemet, så som attt installera programmet ScreenConnect. ScreenConnect användes för att överföra filer från sjukvårdsorganisationerna. ScreenConnect har spårats till en domän som används av *Transaction Data systems* (TDS). TDS är ett ledningssystem för Apotek som används i alla 50 delstater.

## Syfte och frågeställningar

Syfte med rapporten är att undersöka de risker som finns med att koppla upp IoT på internet samt hur dessa enheter kan påverkas av eventuella angripare. Rapporten ska även undersöka vilka eventuella lösningar som kan motverka säkerhetsriskerna med uppkopplad IoT. De frågor som rapporten ska undersöka är:

RQ1: Vilka säkerhetsrisker finns för uppkopplade sjukvårdsenheter?

RQ2: Hur kan säkerhet fastställas för uppkopplade sjukvårdsenheter?

## Metod och material

Denna rapport är en litteraturstudie. Källorna är vetenskapliga artiklar och utgörs av följande artiklar [1-4].

# Resultat

I den första delen av resultatet redovisas några av de säkerhetsrisker som kan uppstå när IoT kopplas upp på internet. I den andra delen redovisas några av de metoderna som används för att förbättra säkerheten hos uppkopplade sjukvårdsenheter. I den sista delen redovisas de olika lagliga implikationerna som kan framkomma vid köp av olika programsårbarheter.

## Säkerhetsrisker

De säkerhetsrisker med uppkopplade IoT lösningar inom sjukvården samlas in i en grupp. En grupp som består av olika typer av cyberattacker [1], [2]. En av dessa attacker är *distributed denial of service* (DDOS). DDOS är en attack där kommunikation mellan enheter helt eller delvis bryts genom att den ena enheten överbelastas. En annan typ av cyberattack mot sjukvårdsenheter är *medjacking*. Här kan obehöriga få tillgång till olika enheter för att sedan ändra doseringar eller funktioner. Vanligast är att dessa enheter kapas för att angripare ska få tillgång till mer centrala system som databaser med mer kritisk information.

År 2008 släpptes en insulinpump med en trådlös kontroll 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. Dessa enheter tillät även i vissa fall obehöriga tillgång till sjukhusets nätverk samt interna system.

## Säkerhetslösningar

För att säkerställa att säkerheten inte fallerar delas säkerhetsåtgärderna in i två olika grupper [2]. Grupp ett är de icke tekniska åtgärderna, medan grupp två består av tekniska åtgärder. Förbättring av de icke tekniska lösningarna görs genom att utbilda 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 behörighets metoder, reservsystem och *Honeypots*.

De olika behörighetsmetoderna är *singlefactor authentication* (SFA), *twofactor authentication* (TFA) och *multifactor authentication* (MFA). Den behörighets metod 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 tredjeparts tjänster eller skanning av specifika fysiska kroppsdelar som iris eller näthinnan. Dessa metoder används för att säkerhetsställa att endast behörig personal kommer åt känslig information [2].

För att minimera påverkan som en DDOS attack kan medföra på livsviktig IoT krävs vissa säkerhetsåtgärder. En säkerhetsåtgärd mot DDOS är användning av reservsystem. Det krävs att det finns reservsystem som kan aktiveras snabbt ifall en uppkoppling inte kan upprätthållas. Detta så enheternas data alltid kan 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 [2].

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

För att IoT enheter 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 validerad och verifierade automatiskt. Det garanterar datasäkerhet och integritet. Kryptografiska hashar tillåter skapandet av unika identifierings koder för olika block. De skapar även spårningsfunktioner till föregående blocks hash. En kryptografisk hashfunktion är en matematisk algoritm som omvandlaar data till en kort kod.

# Diskussion och slutsatser

Denna rapport har tagit fram två risker som kan förekomma med uppkopplade IoT enheter kopplade till sjukvården. Studien påpekar de konsekvenser som säkerhetsriskerna kan medföra samt några säkerhetslösningar som kan implementeras.

## Diskussion

DDOS är en typ av attack som kan medföra stora konsekvenser ifall de inte hanteras korrekt. Tillskillnad från medjacking har DDOS ingenting med att stjäla information från en patient eller sjukvårdsorganisationen. DDOS används för att förhindra kommunikation mellan IoT enheter 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 kopplas till eventuella 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 gå in och ta emot informationen så att personalen kan agera. Användning av alternativa IoT enheter för att skicka informationen medför att om huvudenheten inte skulle kunna skicka data kommer en annan enhet ta över och skicka data till servern.

Medjacking tillskillnad från DDOS handlar inte om att förhindra kommunikationen mellan server och IoT enhet. 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 informationen som skickas till sjukvårdsorganisationen kan vara manipulerad. Med manipulerad information är risken för felaktiga behandlingar mycket större och risken för att andra sjukdomar inte upptäcks ökas. Medjacking kan även leda till att funktioner hos IoT enheter ändras vilket kan innebära ren livsfara. För att fastställa att endast behöriga individer har åtkomst till IoT enheterna bör åtminstone TFA användas om inte MFA. I nuläget är SFA en för svag metod för att säkerhetsställa att rätt individ har åtkomst. Honeypots bör också användas frekvent för att hålla säkerheten uppdaterad för de olika IoT enheterna.

## Slutsatser

Det finns betydligt fler säkerhetsrisker än vad som tagits upp i denna rapport och det är viktigt att känna till. De säkerhetsrisker som tagits upp i rapporten kan få kraftiga konsekvenser. De säkerhetslösningar som tagits fram är mestadels riktade till att motverka de säkerhetsrisker som rapporten tar upp. Dessa säkerhetslösningar är inte specificerade för just IoT utan de fungerar för både IoT och andra uppkopplade system. Framtida arbete och studier kan komma att fokusera på hur implementation av blockkedjor ska används inom IoT för att säkerhetsställa 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: <https://doi.org/10.4108/eai.13-7-2018.155079>

[2] 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: <https://doi.org/10.1016/j.future.2019.12.028>

[3] B. Toulas “Hackers breach healthcare orgs via ScreeanConnect remote access.” *bleepingcompuer.* [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)

[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)