|  |
| --- |
| Rapport |

IoT innom sjukvården

*Underrubrik*

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



Sammandrag

Skriv in abstrakt (ca 200 ord)

Nyckelord

IoT, Sjukvård, Programsårbarhet, Säkerhetsrisker, Säkerhetslösningar

Innehåll

1 Inledning 3

1.1 Syfte och frågeställningar 3

1.2 Metod och material 3

2 Resultat 4

2.1 Säkerhetsrisker 4

2.2 Säkerhetslösningar 4

2.3 Lagliga implikationer vid köp av programsårbarheter 4

3 Diskussion och slutsatser 5

Referenser 6

# 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 på öppet internet, 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.

Marknaden för programsårbarheter kan delas in i två olika typer varav den ena är laglig och den andra olaglig [2]. Programsårbarheter är säkerhetsproblem med olika mjukvaruprogram som tillåter obehöriga åtkomst till information. På den lagliga marknaden delas köpare in i två kategorier, *attackers* (angripare) och *defenders* (försvarare) [3]*.* Försvarare är de individer eller företag som köper programsårbarheter för att förbättra säkerheten i programmet. Angripare är de individer eller företag som köper programsårbarheter för att använda sårbarheterna. Marknaden bygger på att sårbarheten först ges ut till angriparna som sedan får betala för att försvarana ska få information om sårbarheten. Programsårbarheterna säljs för mellan 5 000 och 250 000 dollar beroende på omfattning och användningsområde för sårbarheten.

## 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 de etiska och lagliga dilemman som förekommer vid köp av programsårbarheter. De frågor som rapporten ska undersöka är:

RQ1: Vilka säkerhetsrisker finns för uppkopplade sjukvårdsenheter?

RQ2: Hur kan säkerhet fastställas för uppkopplade sjukvårdsenheter?

RQ3: Vilka lagliga implikationer förekommer när programsårbarheter används?

## Metod och material

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

# Resultat

I den första delen av resultatet redovisas några av de säkerhetsriskerna som kan uppstå när IoT kopplas upp på internet. I den andra delen redovisas några av dem 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 säkerhetsriskerna med uppkopplade IoT lösningar inom sjukvården samlas in i en grupp, denna grupp består av olika typer av cyberattacker [1], [4]. 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 attackerare 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 [4]. Grupp 1 är de icke tekniska åtgärderna, medan grupp 2 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 säkerhetslösningar är multifactor authentication (MFA) skydd mot DDOS. MFA används för att säkerhetsställa att endast behöriga har åtkomst till det system eller den enhet som efterfrågas. MFA är den säkraste av tre olika typer av verifieringsmetoder. Den minst säkra är singlefactor authentication där endast ett lösenord används för att säkerhetsställa att en behörig användare har åtkomst till systemet. Den näst bästa metoden är twofactor authentication där ytterligare en säkerhetsåtgärd är genomförd för att säkerhetsställa att endast behöriga har åtkomst. MFA är den säkraste verifieringsmetoden där flera säkerhetsåtgärder genomförs för att säkerställa att behöriga har åtkomst. För att undvika att DDOS attacker får en stor påverkan på livsviktiga enheter krävs vissa säkerhetsåtgärder. Det krävs att det finns reservsystem som kan aktiveras snabbt ifall en uppkoppling inte kan upprätthållas. Detta så enheternas signaler alltid kan nå behörig och aktuell personal.

## Lagliga implikationer vid köp av programsårbarheter

Skriv dina resultat i förhållande till frågeställning 2 osv.

# Diskussion och slutsatser

# 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] M. J. Wolf och N. Fresco, ”Ethics of the software vulnerabilities and exploits market,” *The Information Society*, vol. 32, no. 4, ss. 269-279, Maj 2016, DOi: <https://doi.org/10.1080/01972243.2016.1177764>

[3] M. Guo, H. Hata och A. Babar, ”Revenue Maximizing Markets for Zero-Day Exploits,” *Autonomous agents and multi-agent sytems,* vol. 35, no. 2, Juli 2021, DOI: <https://doi.org/10.1007/s10458-021-09522-w>

[4] 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>