|  |
| --- |
| Rapport |

Rubrik

*Underrubrik*

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



Sammandrag

Skriv in abstrakt (ca 200 ord)

Nyckelord

IoT

Innehåll

1 Inledning 3

1.1 Syfte och frågeställningar 3

1.2 Metod och material 3

2 Resultat 4

2.1 Underrubrik 4

2.2 Underrubrik 4

3 Diskussion och slutsatser 6

Referenser 7

# 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 bevakas från en dator. IoT är mikrochips som ofta kopplas till sensorer, dess uppgift är att samla samt byta data med varandra. IoT i sjukvården är 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 framkommer när IoT ska kopplas upp på internet. Vid uppkoppling av dessa enheter uppkommer olika säkerhetsrisker. År 2015 hittades 68 000 medicinska system på öppet internet [1]. Dessa enheter var uppkopplade via ett gammalt operativsystem (OS) men flertalet kända säkerhetsproblem. 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]. 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 fixa säkerheten i programmet. Angripare är de individer eller företag som köper programsårbarheter för att använda sårbarheterna. Modellen för marknaden bygger på att sårbarheten först ges ut till angriparna som sedan får betala för att försvarana ska få informationen om sårbarheten. Programsårbarheterna säljs för mellan 5 000 till 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 attacker. Rapporten ska även undersöka de etiska och lagliga dilemman som förekommer inom köp av programsårbarheter. Av dessa anledningar är de frågor som ska besvaras:

RQ1: Vilka typer av säkerhetsrisker finns för uppkopplade sjukvårdsenheter?

RQ2: Vilka etiska dilemman finns på marknaden för programsårbarheter?

RQ3: Vilka lagliga implikationer förekommer när programsårbarheter används?

## Metod och material

Beskriv rapportens metod och material

# Resultat

Metatext

## Underrubrik

Skriv dina resultat i förhållande till frågeställning 1

## Underrubrik

Skriv dina resultat i förhållande till frågeställning 2 osv.

# Diskussion och slutsatser

# Referenser

Skriv in referenser

[1] [eai.13-7-2018.155079 (eudl.eu)](https://eudl.eu/pdf/10.4108/eai.13-7-2018.155079)

[2] [Full article: Ethics of the software vulnerabilities and exploits market (tandfonline.com)](https://www.tandfonline.com/doi/full/10.1080/01972243.2016.1177764)

[3] [2006.14184.pdf (arxiv.org)](https://arxiv.org/pdf/2006.14184.pdf)