Myndigheten
för civilt försvar

2020-06-11 14:00 CEST

# Öka motståndskraften mot ransomware-attacker

**Phishing-kampanjer med covid-19-skepnad eller riktade ransomware-attacker mot sjukvården, har redan observerats och inträffat i andra länder. Därför genomförs nu en särskild informationsinsats mot den svenska hälso- och sjukvårdssektorn där fokus är förebyggande åtgärder mot ransomware.**

I Sverige har både offentlig och privat verksamhet drabbats av ransomware-angrepp det senaste året. Ett angrepp av ransomware skulle kunna slå hårt mot sjukvården, som just nu befinner sig i ett ansträngt läge med anledning av covid-19.

- Phishing-kampanjer eller riktade ransomware-attacker mot sjukvården, har redan observerats och inträffat i andra länder. Dessutom försöker kriminella på olika sätt att utnyttja situationen. Det finns en risk att det även kan inträffa i Sverige och nu genomförs en särskild informationsinsats mot den svenska hälso- och sjukvårdssektorn där fokus är förebyggande åtgärder mot ransomware, säger Hedvig Kylberg, handläggare vid enheten för operativ cybersäkerhet, CERT-SE på MSB.

## Vad är ett ransomware-angrepp?

Ett angrepp av ransomware, kan innebära att hela eller delar av en verksamhets it-system med dess information blir krypterad och inte tillgänglig för medarbetarna. I många fall stjäls även information och sedan hotar angriparna med att publicera den känsliga informationen om inte en lösensumma betalas. Organisationen behöver ha en uppfattning om vilka konsekvenser ett sådant angrepp skulle få för både verksamheten och patientsäkerheten.

## Viktigt med förebyggande arbete

Det är svårt att helt skydda sig från angrepp, men förebyggande åtgärder såsom kontinuerligt it-säkerhetsarbete med bra rutiner för säkerhetskopiering och återställning, samt utbildning av medarbetare, underlättar hanteringen och begränsar skadan. Möjligheten att snabbt kunna återställa it-miljön så att verksamheten kan återgå till normalitet och hålla nere kostnaderna för hanteringen av angreppet, kan göra betydande skillnad. Det är viktigt att även i ett ansträngt läge fortsätta att prioritera säkerhetsunderhåll av it-miljön, även om vissa delar av dessa arbeten kan innebära kortare avbrott i tjänsterna.

## Myndigheternas rekommendationer

Flera myndigheter har tillsammans tagit fram rekommendationer som riktar sig till ansvariga för it-infrastruktur och informationssäkerhet inom hälso- och sjukvårdsverksamhet, beslutsfattare, tekniker och användare av verksamhetens it-system.

Rekommendationerna i Öka motståndskraften mot ransomware ska ses som ett underlag och stöd. Respektive organisation/verksamhet inom hälso- och sjukvårdssektorn ska kunna använda innehållet för riskanalyser, beslutsunderlag, utbildning och kommunikation på det sätt som bedöms vara lämpligt för verksamheten. Exempelvis kan ytterligare målgruppsanpassning av budskapen således behöva göras. Ytterligare stöd i arbetet att öka

motståndskraften mot många cyberhot, finns i rapporten Cybersäkerhet i Sverige – rekommenderade säkerhetsåtgärder. Där presenteras tio åtgärdsområden som bör prioriteras. Rekommendationerna ersätter inte systematiskt säkerhetsarbete.

*CERT-SE är Sveriges nationella CSIRT (Computer Security Incident Response Team) med uppgift att stödja samhället i arbetet med att hantera och förebygga IT-incidenter. Verksamheten bedrivs vid MSB.*

---

Myndigheten för civilt försvar är den ledande, inriktande och samordnande myndigheten i det civila försvaret. Myndigheten säkerställer att samhället är förberett för kris, höjd beredskap och krig.

## Kontaktpersoner

**Myndigheten för civilt försvars presstjänst**
Presskontakt
press@mcf.se
010-240 44 44

**Anna Wennerström**
Presskontakt
Pressansvarig
anna.wennerstrom@mcf.se