Jourhavende i dag: Tanja Parker Astrup
Telefon: 33 47 17 02 – **Mail:** indland@pol.dk

Siden er redigeret/layoutet af:
Kim Frydensberg/Kaspar Busch

Maryam Nazem fik sin computer kapret

Indehaver af skønhedsklinik fik sort skærm på sin computer og blev opkrævet en løsesum efter at have trykket på et link. Hun er et af tusindvis af ofre for ransomware i 2016.

IT-KRIMINALITET

JAKOB SORGENFRI KJÆR

Eksperter inden for it-sikkerhed har døbt 2016 til at være ransomwarets år med henvisning til en eksplosiv stigning i den type cyberangreb, hvor kriminelle tager kontrollen over ofrenes computer for derpå at opkræve løsesum. I det forgangne år var Maryam Nazem og hendes skønhedsklinik, CosmeCare, et af mange danske ofre for ransomware.

Før jul havde indehaveren af den københavnske klinik som de fleste andre erhvervsdrivende ekstra travlt op til højtiden. Maryam Nazem gik og ventede på at få leveret en pakke med posten, da der tikkede en mail ind, som ved første øjekast var fra Post Nord. Postvæsnets velkendte røde logo illustrerede mailen, der oplyste, at »vi har modtaget din pakke«, men »var ude af stand til at levere denne pakke til dig«. Det fremgik, at hun skulle trykke på et link og udskrive en forsendelsesetiket og vise den på posthuset for at få pakken udleveret.

Maryam Nazem havde lidt travlt og skrålæste kun teksten på sin stationære computer. Hun lagde derfor ikke mærke til, at der var flere sproglige fejl i mailen, hvilket er karakteristisk for såkaldte phishingmails.

»Jeg stod præcis og ventede på en pakke og var i en lidt stresset situation i klinikken. Da jeg trykkede på det så kom der helt sort skærm. Jeg prøvede at taste lidt frem og tilbage og forsøgte at lukke programmet, men jeg kunne ingenting. Efter et minut kom der en meddelelse på engelsk om, at alle mine filer var blevet låst, og hvis jeg skulle have dem tilbage, skulle jeg betale for det. Jeg var helt chokeret og vidste slet ikke, hvad jeg skulle gøre«, husker Maryam Nazem.

Myndigheder og sikkerhedsindustrien beretter om en eksplosiv stigning i ransomware de senere år. Selskabet Trend Micro har registreret mere end en halv million angrebsforsøg i Danmark i 2016. Antallet af politianmeldelser om afpresning herhjemme er næsten fordoblet siden 2010. Og en survey fra revisionsselskabet PWC viser, at to ud af tre virksomheder i 2016 har været ramt af ransomware.

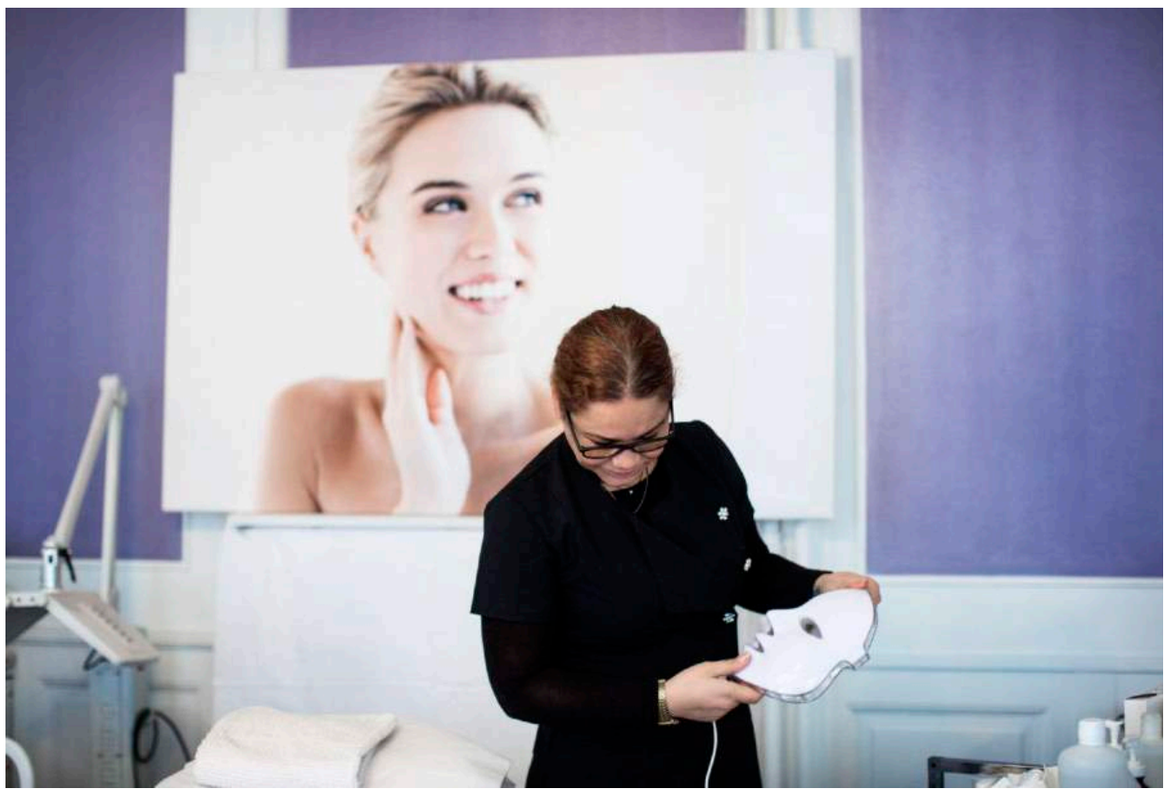
Betal – eller angiv dine venner

Måden at minimere konsekvenserne på er at sørge for at have backup; det vil sige at have gemte kopier af alle sine filer et sted, som er afkoblet fra computeren, så hackerne ikke kan få adgang. Danske Trustbox er en af udbyderne af backup, så hvis en kunde får hacket eller kapret sine systemer, kan offeret slette alt og bagefter få gendannet indholdet.

Trustbox har siden opstarten i 2014 fået over 4.000 kunder, primært fra erhvervslivet, og efterspørgslen er steget i takt med truslen fra ransomware. Partner Claus Elnegaard anslår, at 25-30 procent af kunderne inden for det seneste halvandet år har bedt om at få gendannet deres it-systemer som følge af denne type it-kriminalitet.

»Vi oplever ekstremt mange forskellige former for ransomwaremails, og i mange tilfælde klæder angriberne sig i et velkendt brand. Mange it-brugere føler sig sikre med et antivirusprogram, men det nytter typisk ikke noget, fordi man jo selv kommer til at lukke forbryderen ind ved at trykke på et link. Oftest kræver afsenderne en løsesum, men i nye eksempler har vi set, hvordan offeret kan slippe for at betale ved at angive tre af sine venner«, siger Claus Elnegaard.

Det er lukrativt for hackerne, fordi de fleste af os har paraderne helt nede, når personer, vi har tillid til, sender os links. Og ved at få offeret til at sende aben videre til sine venner kan forbryderne potentielt mangedoble deres indtjening.



LØSESUM. **Lige før jul blev skønhedsklinikken CosmeCare ramt af ransomware. Indehaver Maryam Nazem nægtede at betale løsesummen for at få sine egne filer tilbage, og det har kostet hende tusindvis af kroner og en masse ekstraarbejde.** Foto: Nanna Navntoft

Maryam Nazem anede ikke sine levende råd, da hun blev ramt. I sin klinik foretager hun almindelig hud- og kropspleje, men også mindre plastikkirurgiske behandlinger, der medfører myndighedskrav om at føre detaljerede patientjournaler. Disse journaler havde hun heldigvis backup af, så de var sikret. Men der var en række andre filer – patientvejledninger, arbejdsdokumenter og private dokumenter og billeder – som pludselig var låst for hende.

Maryam Nazem tog kontakt til en it-sagkyndig, der satte hende ind i, hvad hun var blevet ramt af. Rådgiveren anbefalede hende at betale hackerne for at få kontrol over computeren igen. Men han fortalte også om et tilfælde, hvor offeret kun fik halvdelen af sine filer tilbage efter at have betalt.

»Jeg blev arrig, for hvorfor pokker skulle jeg betale til nogle kriminelle – særligt når der ikke er nogen garantier. Det vigtigste for mig var, at jeg havde sikret alle mine patientjournaler. Hvis de også var røget, var jeg nok endt med at betale løsesummen, for ellers skulle jeg formentlig lukke min butik. Det var da superærgerligt at miste alle de andre filer, men jeg tænkte: Fuck det«, siger Maryam Nazem.

Hun besluttede sig for at hyre en anden it-rådgiver, der hjalp hende med at rense computeren, slette indholdet og starte helt forfra. Hun fandt aldrig ud af, præcis hvor meget hun skulle have betalt hackerne, men andre, der blev ramt af de mange falske Post Nord-emails, blev afkrævet et beløb på omkring 3.500 kroner.

Har bebrejdet sig selv

Maryam Nazems omkostninger ved angrebet har været større end løsesummen – i alt cirka 8.000 kroner for et nyt program og it-rådgivning.

»Min virksomhed er først ved at komme på benene igen nu. Jeg har ikke kunnet slappe af og har haft en masse overarbejde i et par måneder, fordi patienterne jo hele tiden kommer og går og skal have informationer, som jeg har skullet genskabe«, siger Maryam Nazem.

Mange gange har hun bebrejdet sig selv for at have trykket på den falske mail.

»Jeg har tænkt: Ih, hvor var det dumt – men man er jo bare et menneske. Og forskrækkelsen sidder stadig i mig; jeg er helt mistænkelig over for alle mails, og jeg er begyndt at ringe til folk, når de sender links – »er det rigtigt, at jeg skal trykke der, og at det her kommer fra dig««, fortæller Maryam Nazem.

Desuden er hun begyndt at have to slags backup af sine systemer, hvilket tager hende en halv time ekstra hver aften efter lukketid. Den ene backup lagres automatisk i skyen gennem et Microsoft-produkt, hun har investeret i. Den anden backup lægger hun manuelt over på en ekstern harddisk, som ellers ikke er tilkoblet computeren.

På den måde har Maryam Nazem handlet helt i tråd med de vigtigste råd fra politiet og sikkerhedseksperter: Betal ikke forbryderne, og lav både automatisk og manuel backup af dine systemer.

jakob.sorgenfri@pol.dk

GODE RÅD

SÅDAN SIKRER DU DIG

Europæisk politi og sikkerhedsbranchen har lavet hjemmesiden nomoreransom.org for at forebygge og hjælpe ofre for ransomware. De vigtigste råd til it-brugere er:

- Lav backup af dine systemer på en måde, så ransomwaren ikke kan få fat på kopierne af dine personlige data.
- Opdater din software. Installer straks en ny version af et styresystem, og sig ja til automatiske softwareopdateringer.
- Brug et robust antivirusprogram for at beskytte dine systemer mod ransomware.
- Stol ikke på nogen. Skadelige links kan blive sendt til dig fra venners kompromitterede mail- eller sociale mediekonti. Kriminelle sender ofte falske e-mails, der ligner dem fra en kendt netbutik, banken, politiet, Skat eller andre myndigheder.