DIGITAL AFPRESN

Flere og flere bliver ofre for it-kriminelle, der låser data og kræver løsepenge – problemet har udviklet sig til en reel epidemi, siger ekspert

AFPRESNING

Lars Lindevall Hansen | larh@bt.dk

Et særdeles lukrativt marked for professionelle it-kriminelle er i den seneste tid vokset eksplosivt.

Både private og erhvervsdrivende bliver i stigende grad ramt af datakidnapning – såkaldt ransomware – viser nye tal.

Det foregår ved, at hackere skaffer sig adgang til computere og servere – hvorefter de krypterer data og kræver, at ejeren betaler løsepenge for at få en 'nøgle', der kan låse filerne op.

For virksomheder kan det f.eks. dreje sig om regnskaber eller kundekartoteker, og for private handler det typisk om billeder, videoer og andre personlige dokumenter.

Ofte inficeres ofrets computer, fordi han eller hun har åbnet en fil eller et link, der aktiverer virussen. Det kan dog også ske, hvis man besøger usikre hjemmesider.

Peter Kruse, der er en af landets førende eksperter i it-kriminalitet, kalder problemet for en 'epidemi'.

»Sidste år tog det for alvor fart. I 2017 er der kommet endnu flere varianter, og det er nu både en reel epidemi og en industri,« siger Peter Kruse, der er specialist i sikkerhedsfirmaet CSIS Security Group.

Organiseret kriminalitet

It-sikkerhedsfirmaet Trend Micro Danmark, der overvåger udviklingen, registrerede i andet halvår af 2016 hele 382.425 forsøg på ransomware-angreb blandt danske kunder – det gælder både private og virksomheder. Det er en stigning på 157 procent sammenlignet med første halvår. Firmaet har dog ikke det fulde overblik og formoder, at det reelle omfang er langt større.

CSIS Security Group registrerede 554 hændelser i 2016, hvor danske virksomheder fik blokeret data med krav om løsepenge. Der er også her

For at skræmme ofrene til at betale hurtigt skriver de nogle gange, at der eksempelvis er børneporno eller andre ulovlige filer på computeren. De kan også finde på at bruge et falsk politilogo, så folk bliver enormt bange og betaler med det samme

Peter Kruse, specialist i sikkerhedsfirmaet CSIS Security Group

tale om en stigning på 71 procent, hvis man sammenligner sidste år med 2015.

»De har organiseret det på den måde, så de meget nemt kan trække penge ud af folk, fordi de ved, at de rammer dem dér, hvor det gør allermest ondt,« siger Peter Kruse.

En tidligere rapport fra Digitaliseringsstyrelsen viser desuden, at otte procent af danskerne har været udsat for skadelig software, der forsøger at spærre for adgangen til data og programmer.

Et af problemerne er, at det indbringende marked kan tiltrække mindre dygtige it-kriminelle, der ikke nødvendigvis er i stand til at genskabe data, påpeger Claus Elnegaard, der er partner i firmaet Trustbox, som er leverandør af cloudbaseret backup til både private og virksomheder.

»Der er nogle it-kyndige kriminelle, der har lavet programmerne, som andre kriminelle bare genbruger. Det er som regel relativt simple programmer, men i værste fald kan de stadig ødelægge dine filer eller lukke din virksomhed,« siger Claus Elnegaard.

Grovere metoder

I den seneste tid er hackernes metoder blevet langt mere grove, forklarer Peter Kruse.

»For at skræmme ofrene til at betale hurtigt skriver de nogle gange, at der eksempelvis er børneporno eller andre ulovlige filer på computeren. De kan også finde på at bruge et falsk politilogo, så folk bliver enormt bange og betaler med det samme,« forklarer Peter Kruse.

Beløbene, som de it-kriminelle kræver for at åbne computeren, ligger typisk på mellem 1.500 og 2.000 kr. Det er en bevidst strategi, at beløbet ikke er højere, så folk ikke gør en sag ud af det, men blot betaler.

For virksomheder kan det dog godt være langt højere beløb, hvis hackerne ved, at de sidder på værdifulde data. Og der kan ryge 'dummebøder' oveni, hvis ikke pengene er overført inden for et bestemt tidsrum, f.eks. 48 timer.

Låser også backup

Peter Kruse forklarer, at ransomware er blevet langt sværere at forhindre – og slippe af med – når ens computer er blevet inficeret. Senest er hackernes værktøjer blevet så avancerede, at de også kan få adgang til backup-systemer.

»De er langt mere raffinerede, end de var til at begynde med. De går efter alle de drev, der er tilgængelige i netværket, og de er også blevet i stand til at opsnappe og misbruge brugernavne og password til backup-systemer.«

SÅDAN BESKYTTER DU DIG MOD RANSOMEWARE

1: Brug en ekstern harddisk, som du kun har tilkoblet computeren, når du skal bruge filerne. Hvis du har en server til backup, der konstant er tilkoblet din computer, er der også risiko for, at den kan blive inficeret.

2: Sørg for at holde alle dine computer-programmer og styresystemer opdaterede. Et program, der er særligt sårbart, er Adobe Flash.

3: Lad være med at åbne filer, som virker tvivlsomme. Postfirmaet eller banken vil ikke normalt sende dig en ZIP-fil. Besøg ikke hjemmesider og tryk ikke på links, som du ikke har tillid til.

4: Hold dig fra konkurrencer og diverse spil, der f.eks. dukker op på Facebook.

5: Lad være med at bede computeren om at huske passwords og brugernavn – skriv det hellere manuelt hver gang.

6: Sørg for at have et antivirus-program på din computer. Der findes flere gratis programmer på nettet.

7: Sørg for at sikkerhedskopiere dine filer jævnligt og gerne flere forskellige steder.

8: Betal ikke. Alle eksperter og myndigheder er enige om et råd: Betal ikke, hvis dine data bliver låst – det vil kun øge interessen for ransomware blandt kriminelle og forstærke problemet.

Kilder: CSIS, Trustbox

ING BOOMER

● Et øjeblik efter at Lars Henneberg havde trykket på mailen, han troede var fra PostNorden, var hans filer krypteret. I en besked på skærmen krævede den eller de kriminelle 4.000 kr. FOTO: IRIS

'Jeg følte mig magtesløs

Lars Hennebergs stilladsfirma fik krypteret filerne

Jeg tør næsten ikke tænke på, hvis jeg ikke havde haft backup. Det ville have været belastende for mine kunder, krævet et stort stykke arbejde og betydet en masse mistede billeder og filer

Lars Henneberg

ANGREBET

Lars Lindevall Hansen | larh@bt.dk

Lars Henneberg er blandt de danskere, der har oplevet at blive afpresset af it-kriminelle.

Hans firma, Henneberg Stilladser i Hillerød, blev i sommeren 2016 ramt af et ransomware-angreb.

»Jeg fik en mail fra PostNord om en pakke, jeg skulle hente. Jeg havde ikke bestilt noget, men det kunne andre i familien eller virksomheden jo have gjort, så jeg åbnede mailen. Der stod et pakkenummer, og alt så fint ud. Der var ikke meget tekst, og derfor tænkte jeg ikke over, at der kunne være noget galt. Så klikkede jeg på linket uden at tænke mere over det,« siger 46-årige Lars Henneberg.

Et øjeblik senere var alle hans filer blevet krypteret. Han kunne åbne dem, men indholdet var volapyk. En besked dukkede op på skærmen: Han havde 48 timer til at betale ca. 4.000 kr., og ellers ville hans filer blive slettet.

»Jeg følte mig magtesløs, for det hele gik i stå. Mit firma var nede at ligge i en uge, hvor jeg hverken kunne fakturere eller betale regninger.«

Tæt på at betale

Han forklarer, at han var på nippet til at betale for at få sine filer igen.

»Men så tænkte jeg 'ej, det gider jeg sgu ikke. Så ender jeg med at støtte de kriminelle'.«

For Lars Henneberg betød mødet med ransomware, at han måtte købe en ny pc for at undgå virus, der måske stadig lå på den inficerede pc. Heldigvis havde han en cloud-baseret backup-tjeneste, så han kunne få genskabt data. Det tog dog en uge, før det hele fungerede igen.

»Jeg tør næsten ikke tænke på, hvis jeg ikke havde haft backup. Det ville have været belastende for mine kunder, krævet et stort stykke arbejde og betydet en masse mistede billeder og filer.«

Irak bomber IS-leders hus

● Irakiske kampfly gennemførte i weekenden luftangreb mod et hus i Anbar i Irak, hvor lederen af Islamisk Stat, Abu Bakr al-Baghdadi, formodedes at opholde sig. I december forhøjede USA dusøren for oplysninger, der kan pege i retning af IS-lederen, til hvad der svarer til 175 millioner danske kroner. */ritzau/*

Koldt hav stopper olien

● Det kolde hav nordøst for Fyns Hoved har sat en stopper for et olieudslip fra containerskibet 'Victoria'. Skibet berørte grund nordøst for Fyns Hoved fredag, og det resulterede i en 50 meter lang og 20 centimeter bred flænge i skibet. Der er efterfølgende fundet olie flere steder – også på den nordfynske kyst – men udslippet fra skibet er nu stoppet, lyder det fra vagtholdslederen hos Forsvarets Operationscenter. »Det olie, der er i tanken, er heavy fuel. Når vandet er fire grader, er oliens konsistens som asfalt,« siger han. */ritzau/*

Erdogan vil oprette sikre zoner i Syrien

● Bahrain. Tyrkiets præsident, Recep Tayyip Erdogan, vil skabe en sikker zone i Syrien på mindst 4.000 eller 5.000 kvadratkilometer. Zonen vil kræve en ikke-flyve zone.

Det skal ifølge Erdogan ske i forbindelse med udvidelse af Tyrkiets militære operationer i Raqqa og Manbij.

Erdogan siger, at Islamisk Stat om kort tid vil være nedkæmpet i byen al-Bab.

Det er den sidste by i regionen, hvor Islamisk Stat har fodfæste. */ritzau/Reuters*