TDC Erhverv

Sådan beskytter du din virksomhed mod Ransomware

Sådan beskytter du din virksomhed mod Ransomware

Ransomware problemet

Allerede nu dobbelt så mange angreb som i hele 2016

Mange virksomheder har stiftet bekendtskab med Ransomware i det forløbne år og problemet ser desværre ud til at blive større og større. Således er mange virksomheder verden over for nyligt blevet ramt af "WannaCry" Ransomware angrebet. Men Ransomware er ikke noget nyt fænomen og allerede den 6.marts 2017 kunne vi i Computerworld læse at "Selv om vi kun er tre måneder inde i 2017, har der allerede været over dobbelt så mange Ransomware-angreb som i hele 2016".

Center for Cybersikkerhed beretter ligeledes i deres publikation "Cybertruslen mod Danmark februar 2017" at "Ransomware er en af de mest fremtrædende trusler inden for cyberkriminalitet."

"Hackerne bruger meget ofte phishing og social engineering til at få folk til at klikke på links i e-mails, sms'er eller på reklamebannere, der installerer Malware. Den menneskelige faktor er derfor af stor betydning, hvis man vil undgå at blive offer for Ransomware.".

Baggrund for udviklingen

Denne udvikling skyldes bl.a. at det er nemmere for cyberkriminelle at få fat i værktøjer der kan benyttes til deres angreb, samtidig med at disse værktøjer ikke længere kræver specielle færdigheder, men kun kræver viljen og hensigten til at benytte dem.

Således ser vi at Ransomware værktøjerne både bliver benyttet målrettet mod bestemte virksomheder, men også i kampagner hvor angrebene rammer bredt og mere eller mindre tilfældigt.

"Advanced Persistent Threat (APT-angreb) kan være den virkelige årsag til angrebet."

Vi har set eksempler på Ransomware angreb, hvor det efterfølgende har vist sig at Ransomware angrebet blot var det sidste led i "exploit kæden", og at den virkelige årsag til angrebet var et såkaldt APT-angreb.

APT-angreb er avancerede cyberangreb, der er målrettet imod en bestemt og nøje udvalgt virksomhed, som har til formål at kompromittere og/eller stjæler virksomhedens intellektuelle værdier. Efter succesfuldt at have trukket informationer ud af virksomheden over en længere periode og egentlig have fuldendt angrebet vælger hackerne, i nogle tilfælde, til sidst også at kryptere data for at afkræve løsepenge.

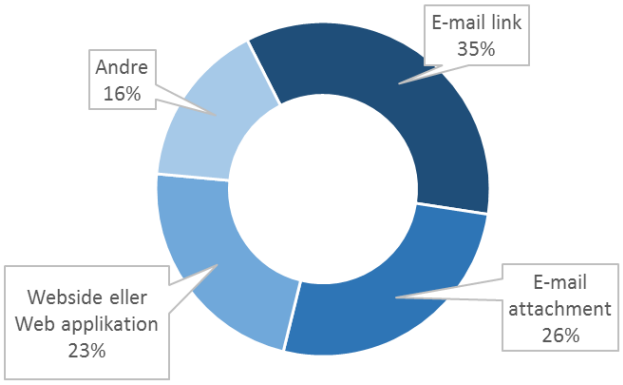
Angrebsvektorer afslører de svage punkter

Alle analyser peger på at de primære angrebsvektorer der bliver benyttet til at inficere IT systemer er e-mails og sårbarheder i applikationer.

Således viser Ostermans research Inc.'s Ransomware analyse fra 2017 også at:

- I 61% af tilfældene blev links eller vedhæftede filer i e-mails benyttet som primær angrebs vektor.
- I 24% af tilfældene blev sårbarheder i websider benyttet.
- I 17% af tilfældene benyttes andre angrebsvektorer der fordeler sig på Social Media 4%, USB Stik 3%, forretningsapplikationer 1% og andre 9%.

Undersøgelsen viser, at i 42% af tilfældene havde Malware spredt sig til flere endpoints efter at have fået adgang til IT systemerne og dermed forvoldt endnu større skade.



Hvorfor fanges disse angreb ikke af vores Firewalls og Anti-virus beskyttelse?

Traditionel beskyttelse såsom anti-virus og firewalls er stadigvæk vigtige i beskyttelse mod Ransomware. Men da disse typisk er signaturbaserede er de ikke længere tilstrækkelige. De fanger nemlig kun allerede kendte trusler og har ingen eller meget ringe effekt ved ukendt Malware, der i dag er forholdsvis nem at fremstille og derfor benyttes i stigende grad.

For at opbygge et effektivt forsvar skal der benyttes mere proaktive løsninger og teknologier som findes i Next Generation Firewalls kombineret med endpoint løsninger med "Sandbox teknologi".

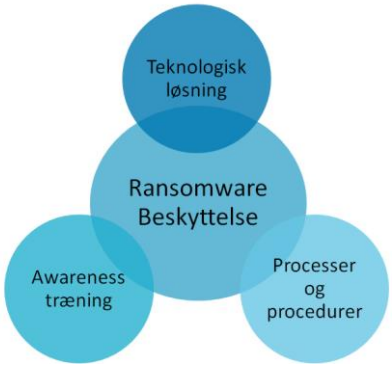
Sandboxing emulerer ukendte filer i et kontrolleret miljø, for at undersøge om der skjuler sig ondsindet kode som kan eksekveres. Skulle dette være tilfældet sættes filen enten i karantæne alternativt fjernes den ondsindede kode i filen før den sendes videre, ved hjælp af teknologier som eksempelvis advanced threat extraction.

Hvordan kan TDC hjælpe med at beskytte min virksomhed mod Ransomware angreb?

Ligesom med de fleste IT sikkerhedsmæssige udfordringer kan effektiv Ransomware beskyttelse ikke opnås med et enkelt produkt eller en enkelt proces alene.

Da den primære angrebsvektor i forbindelse med Ransomware angreb er Phishing e-mails rettet imod virksomhedens medarbejdere vil det bedste forsvar mod Ransomware angreb altid være kombination af de rette teknologiske løsninger, nødvendige processer og procedurer samt at have kontinuerlig fokus på Awareness træning af brugere.

Vores ydelser er bygget op omkring nedenstående 5 faser, som er centrale områder at forholde sig til hvis man ønsker at etablere effektiv Ransomware beskyttelse.



Fase 1 "Forebyggelse"
Sikring mod angreb og træning af brugere

- Awareness træning af brugere i form af Phishing mail kampagner og undervisning
- Risk assessment af IT-systemer –herunder
  - Sårbarhedsskanning af netværket
  - Pentests for at klarlægge svage punkter i netværket
- Automatiseret proces for Backup af data
- Implementere forsvar baseret på Anti-Ransomware teknologier samt Sandboxing løsninger for at opnå effektiv beskyttelse imod ukendt Malware
- DNS baseret sikkerhed, som bl.a. forhindrer besøg på websider med skadeligt indhold.

Fase 2 "Opdagelse"
Monitorering af datatrafik og hændelser

- Benytte Sandboxing og Anti-Ransomware løsninger til at detektere og stoppe eksekvering af skadelig kode i Malware
- Detektere potentielle angreb inden de rammer netværket
- Opdage potentielle angreb inde i netværket evt. ved at kunne detektere Command and Control trafik.

Fase 3 "Bekæmpelse"
Identifikation, isolering og bekæmpelse

- Hurtig afgrænsning af effektiv bekæmpelse af Ransomware angrebet
- Forhindre Ransomware i at kommunikere med Command and Control serveren ved "bot detection" og "blocking".

Fase 4"Genoprettelse"
Genskabe data og genoprette betroet tilstand

- Genskabe de krypterede filer for at minimere påvirkningen af angrebet
- Udnyt "forensics data" til at afgøre om truslen er helt og fuldt elimineret.

Fase 5 "Analyse"
Analyse, evalueringer og rapportering

- Analysere hændelsen med henblik på at afdække hvor og hvordan Malware kom ind i netværket, og hvordan den spredte sig i netværket
- Analysere hvor effektiv forsvaret viste sig at være
- Udarbejde rapport med opnået viden og anbefalinger til, hvad der kan forbedres i det samlede forsvar, således at den samlede sikkerhedsløsning forbedres.

Hvilke producenter benytter TDC til Ransomware beskyttelse

TDC benytter markedets førende producenter til Ransomware beskyttelse

TDC benytter de bedste teknologier fra de førende producenter og tilpasser normalt vores løsninger så de imødekommer kundens design og den aktuelle problemstilling hos kunden og ikke en specifik producents produkter.

Vi tilbyder således også Sandboxing løsninger fra forskellige producenter, både på Next Generation Firewalls, i netværk og på endpoints, men i forbindelse med Ransomware beskyttelse vil vi fremhæve to producenter som vi har specielt gode erfaringer med.

I sortimentet fra henholdsvis Check Point og Cisco findes løsninger som på mange områder er ganske unikke og som er velegnede til beskyttelse mod Ransomware angreb.

CHECK POINT SandBlast ZERO-DAY PROTECTION

Check Point leverer fremragende løsninger baseret på deres Next generation Firewalls med SandBlast og SandBlast Agent. SandBlast Agent beskytter helt ud til endpoints og er bygget op omkring deres Advanced Threat Prevention teknologier: Threat Emulation, Threat Extraction, Zero Phishing og Anti Ransomware.

CISCO AMP Threat Grid

Cisco har implementeret deres løsning Advanced Malware Protection (AMP) på tværs af deres mange forskellige enheder på netværket, helt ud til endpoints, som indbyrdes kommunikerer og udveksler informationer i flere uafhængige benchmarks opnår Cisco Breach Detection fremragende resultater.

Beskyttelse i skyen

Begge producenter har intelligente Cloud baserede løsninger som både beskytter vores kunder når de er på farten men samtidig fungere som første forsvarslinje imod Ransomware angreb.

Løsningerne fungerer på DNS niveau og beskytter allerede inden potentiel skadelig trafik kan ramme virksomhedens netværk og blokerer således angrebene i skyen. Løsningerne giver bl.a. mulighed for beskyttelse mod kendte og ukendte websider som hoster Command & Control Server og Call-back aktivitet (Botnet).

Threat Intelligence

Helt unikt for begge producenter er deres meget store Globale Threat Intelligence organisationer, hvor millioner af Malware og sikkerheds hændelser dagligt analyseres og rates. Resultater fra dette analysearbejde sendes umiddelbart videre til alle deres respektive enheder, således at vores kunder altid er beskyttede med de den nyeste viden omkring Ransomware og anden Malware.

Sandboxing

Begge producenter har avancerede Sandboxing løsninger hvor filer eksekveres og emuleres i et beskyttet miljø. Sandboxing løsningerne kan enten undersøge filerne i skyen eller i dedikerede enheder for derigennem at sikre at Malware ikke slipper igennem.

Kontakt os

Der ikke findes én enkelt proces eller ét enkelt produkt, der kan løse alle de sikkerhedsmæssige udfordringer man som virksomhed står overfor i dag, men TDC Erhverv hjælpe dig med klare og operationelle anbefalinger og løsninger til hvordan du optimerer dit forsvar imod Ransomware angreb.

Kontakt vores sikkerhedseksperter på **raadgivning@tdcsikkerhed.dk** og lad os hjælpe dig med at bringe jeres Ransomware beskyttelse up to date. Eller kontakt os for en on-site demo af løsningerne.