2018

Skadelig Programvare – Farer, Forhåndsregler og Tiltak

Kandidatnummer.: 15144

UNIVERSITETET I OSLO | IN2120

Innhold

Innledning

Sannsynligvis kjenner de fleste til begrepet «datavirus». Enten har man hørt det i politikken, lest om det i en avis, eller kanskje man selv har opplevd å bli rammet av et virus. Det man gjerne omtaler som virus kan komme i mange former, og et fellesbegrep for disse formene er «skadelig programvare.» Det er viktig for enhver bruker av datamaskiner og internett å være opplyst om farene ved forskjellige typer skadelig programvare. Jeg skal derfor ta for meg hvilke former noen av de mest kjente skadelige programvarene kan ta, og hvordan de virker, både i teorien og i praksis. All skadelig programvare har opphav i menneskeskrevet kode. Personer som skriver og distribuerer denne koden kalles Hackere. Uten hackere ville det ikke fantes noen former for skadelig programvare. Derfor skal jeg i denne teksten diskutere hvordan en hacker opererer, og samtidig rette fokus mot skaden enkelte hackere har klart å utrette. Til slutt skal jeg ta for meg hvilke tiltak en bruker selv kan ta for å forberede mot og håndtere skadelig programvare.

Hva er skadelig programvare?

Til å begynne med er det viktig å danne seg et godt bilde av hva en skadelig programvare er. Det finnes flere forskjellige definisjoner av en skadelig programvare, men kort oppsummert er skadelig programvare programmer som «*utfører uventede eller uautoriserte handlinger*»[1]. Det vil si programvare som ufrivillig installeres på en enhet med hensikt å gjøre skade. Altså omfatter ikke skadelig programvare bare datavirus, men også flere andre typer trusler. De mest vanlige, som jeg også skal ta for meg er «fork-bomber», «ormer», «trojanske hester», «løsepengevirus», «Spionvare», «logiske bomber», og «rootkits».

Datavirus

Nå som vi har etablert at skadelig programvare ikke bare omfatter datavirus, må vi vurdere hva som kjennetegner datavirus i forhold til andre typer skadelig programvare. Cambridge Dictionary definerer datavirus som «*a computer program or part of a computer program that can make copies of itself and is intended to prevent the computer from working normally*»[2]. En vanlig misforståelse er at et datavirus er en syntetisk variant av virus man finner i naturen. At det er en fysisk organisme som formeres og sprer seg gjennom nettverket eller strømkablene. I realiteten er virus ikke annet enn kodesnutter som enhver programmerer og hacker kan utnytte dersom han har tilstrekkelig kunnskap angående området. Slik som med virus i biologien, er datavirus laget for å formere seg gjennom en vertsenhet og blir et

[1] Hentet fra http://www.betydning-definisjoner.com/Skadelig%20programvare
[2] Hentet fra https://dictionary.cambridge.org/dictionary/english/virus

eksponentielt større problem dersom de ikke fjernes så fort de blir oppdaget. Man bruker derfor ordet datavirus på grunnlag av at kodens fundamentale formeringsmønster minner om biologiens virus sitt formeringsmønster.

Fork-bomber

De aller minste virus-implementasjonene trenger ikke bestå av mer enn én linje. Disse typene virus kalles «Fork-bomber», og er laget for å kjøre en evig prosess som spiser opp alle systemressursene. «Fork-bomber» er en variant av Tjenestenektangrep, på engelsk «Denial-of-Service.» Tjenestenektangrep hindrer de rammede å ta i bruk deler av systemer som de ellers skal ha tilgang til. Dette brukes for eksempel av hackere som ønsker å begrense spesifikke enheter, og deretter utnytte dem til egen fordel. En av de korteste fork-bombene vi kjenner til ble laget for Linux sin kommandolinje, og kan inneholde så lite som 11 tegn, nemlig «:(){:|:&};:». Denne koden vil alene kunne sakke farten til, og eventuelt krasje et system ved å tappe den for ressurser.

Ormer

En type skadelig programvare som også omtales som en variant av virus er ormer. Ormer trenger ikke nødvendigvis bare én vert, slik som vanlige datavirus gjør, men ellers opptrer de veldig likt. Spesielt med ormer er at de tar i bruk et datanett for spredning over flere potensielle enheter. Dette skiller dem fra vanlig virus, som gjerne bare gjør skade på en enhet. Både ormer og virus har ekstra funksjoner som er ment å gjøre skade på enheten, kalt nyttelast (payload på engelsk). Det kan bety at både ormer og virus i noen tilfeller kan være harmløse. Ofte kan nyttelasten i seg selv gjøre stor skade, eller installere andre typer skadelig programvare som har funksjoner utenom selve spredningen.

Trojanske hester

Begrepet «trojansk hest» ble først introdusert etter at grekerne lurte motstanderne sine under den trojanske krigen. De bygget en gigantisk hul tømmerhest og ga den til fiendene i Troja som en gave. Innbyggerne i byen tok imot gaven, uvitende om at grekerne hadde fylt hesten opp med soldater. Senere samme kveld krøp soldatene ut av hesten og angrep byen. På denne måten hadde de greske soldatene klart å infiltrere byens forsvarsmurer, som ledet til at de senere vant krigen. På samme måte som den historiske trojanske hesten, forsøker trojanske hester i datasikkerhet å fremstå som noe positivt, men er i realiteten svært skadelig for enheter. Dette er en en av de enkleste metodene å lure uvitende brukere til å laste ned et skadelig program på egen pc. Den skadelige programvaren er maskert og kan virke prikk lik

programvaren man egentlig ønsket å anskaffe. De spres gjennom falske nettsider, e-mailer, filer og programmer, og er svært vanskelige å oppdage før det er for sent.

Løsepengevirus

Løsepengevirus er en form for virus som ofte spres via Trojanske hester. Denne typen virus skiller seg fra andre typer virus ved at den ikke prøver å skjule at enheten har blitt infisert. Tvert imot, forteller den brukeren om infeksjonen. Derfra krever hackeren løsepenger for å selv fjerne infeksjonen. Et slikt tilfelle kan ofte sammenliknes med en gisselsituasjon. Viktige funksjoner eller filer på enheten blir tatt gissel og låses bak en form for betalingsmur. Avanserte former former for løsepengevirus kan i tillegg kryptere filer. Hackere krever da kompensasjon for å dekryptere dem. Brukeren kan derfra velge å betale hackeren den angitte summen, og få tilbake normal funksjon på enheten. Uansett vil det ofte være mulig å reversere problemene selv. Dette forutsetter at man har tilstrekkelig kunnskap om virusets funksjon, og generell datateknologi.

Logiske bomber

En «logisk bombe» er en variant av trojansk hest som inneholder enda en funksjon som gjør det vanskeligere for brukeren å forstå at noe er galt på enheten. Logiske bomber er nemlig innstilt for å gå av ved et forhåndsbestemt tidspunkt, eller ved andre omstendigheter. Logiske bomber kan derfor i teorien ligge inne på en enhet i flere måneder før den begynner å kjøre den skadelige programvaren. Dette kan forvirre en bruker, og lure han til å for eksempel tro at det er noe han selv gjorde som førte til at enheten ble infisert.

Spionvare

Trojanske hester i seg selv er ufarlige hvis man klarer å unngå dem, men så fort de har infiltrert en enhet, vil de kunne gjøre skade. En av de mer skumle sidene ved en slik infiltrasjon er at man ikke alltid vet om enheten er infiltrert. Spionvare er en form for skadelig programvare som gjemmer seg, og logger flere ting en bruker gjør på enheten. En rutinert hacker vet at etter kort tid vil brukere taste inn sensitiv informasjon, besøke private kontoer, og surfe på enkelte nettsider. Hvis en hacker kan få tak i denne informasjonen, vil han bruke dette for utpressing, identitetstyveri, spionasje eller svindel. En tastelogger er en variant av spionvare som for eksempel vil lagre alt en bruker skriver på tastaturet. Tasteloggere kan også ha muligheten til å ta skjermbilder av skjermen slik at hackeren kan ha full kontroll over brukerens aktiviteter og bevegelser. I veldig alvorlige tilfeller kan hackere få uautorisert tilgang til webkamera og mikrofon, og får dermed enda større innsikt i brukerens private samtaler og bilder.

Rootkits

Mange vil omtale «rootkits» som en av de farligste typene skadelig programvare. Dette er fordi det, slik som andre typer spionvare, kan forbli usynlig på enheten. Rootkits har også uendelig mange forskjellige bruksområder, ettersom de er laget for å kunne gi en hacker full administratortilgang til alle ressurser på en enhet. Basert på hvor avansert en rootkit er, kan hackere i teorien gjøre akkurat som de vil inne i filsystemer, på nettet og i andre programmer gjennom administratortilgangen til enheten. Hvis man først har fått en slik tilgang, er det lett å videre laste ned mer skadelig programvare slik at det tilfredsstiller alle hackernes behov. Det er for eksempel mulig å lekke informasjon, og få det til å virke som om brukeren selv var ansvarlig for lekkingen. Det er i tillegg svært vanskelig å oppdage rootkits på enheter. Et typisk symptom på at en enhet er infisert av rootkits er at innstillinger endres uten brukerinteraksjon. For eksempel kan antivirusprogrammer nekte å kjøre. En annen litt mer avansert metode for å detektere rootkits, er å se på nettverkstrafikken. Dersom bruken er høy til tider hvor den egentlig skal være minimal, kan det være grunn til bekymring.

Hva er en hacker?

Nå som vi har en bredere forståelse av hvordan forskjellige typer skadelig programvare virker, kan vi dykke dypere inn i hodet til en hacker. Hvilke drivkrefter som motiverer hackeren til å bryte loven, og hvordan hackere klarer å lure brukere til å trå i fellene de legger ut. Hvis man vet hvordan en hacker tenker, vil man enklere kunne unngå å selv bli målet deres. Hackere er som regel flinkere og mer erfaren en en gjennomsnittlig bruker når det kommer til programmering, nettverk og datamaskiner generelt. Dette betyr uansett ikke at alle hackere er genier innen området. Faktisk skriver bare et fåtall av hackere egen kode. Mange kan være barn og ungdommer som kjører kode de ikke selv forstår, men som andre programmerere har skrevet og publisert på nettet. Definisjonen av en hacker er kanskje overraskende for mange. En «hacker» er ifølge Store Norske leksikon «*en person som er i stand til å løse problemer og utfordringer ved hjelp av informasjonsteknologi på svært kort tid.*»[3] Altså er de færreste av alle hackere ute etter å gjøre skade på andres enheter. De fleste ser på hacking som en hobby. Det kan sammenliknes med sportsfiske. Hackere ser etter nye og mer komplekse programmer og systemer for å trenge seg gjennom dem. Dette gjør de fleste for mestringsfølelsen alene. På samme måte ønsker fiskere å se hvem som får den største og fineste fisken uten å slakte og spise av den. De flinkeste hackerne blir også søkt ut av organisasjoner for å kvalitetssikre programmene og sikkerheten deres. Slik kan de få

[3] Hentet fra https://snl.no/hacker

oversikt over svakheter og hvilke tiltak som må tas i etterkant. Et mer veldefinert begrep på en person som driver kriminell hacking, nemlig «cracker», dukket da opp for å skille mellom dem og vanlige hackere. I denne teksten omtaler jeg både «cracker» og «hacker» som hacker, for å unngå forvirring.

Drivkreftene til en hacker

Tidligere var den eneste måten å spre skadelig programvare på gjennom fysiske disketter man satt inn i datamaskinen, noe som ikke var en særlig effektiv metode for kriminelle hackere. I dag kobler vi alle enhetene våre opp på internett, hvor vi laster ned alt vi føler vi trenger å laste ned. Dette har skapt et enormt marked for kriminelle organisasjoner. Organisasjonene leier inn hackere til å stjele sensitiv og personlig informasjon, korruptere data, og ødelegge for andre brukere. Informasjon er verdifullt, ofte uvurderlig. Desto mer sensitiv informasjonen er, desto høyere er summen hackere kan bli betalt for anskaffelsen av den. Økonomisk vinning er en av de mest motiverende faktorene for en hacker. Hackere jobber som regel aldri alene, og opererer ofte i små hackergrupper. Dersom en hacker får til noe avansert, vil han også oppnå popularitet blant andre hackere i gruppen. Denne popularitetet kan også være en sterkt motiverende faktor for å fortsette å rebellere og vise seg fram. Som tidligere nevnt, kan informasjonen hackere henter utnyttes for spionasje, utpressing, identitetstyveri og svindel. Selv om det finnes strenge lover mot denne typen informasjonshenting, er hackere, som innbruddstyver, eksperter på å skjule sporene sine. I tillegg har hackere fordelen at de kan befinne seg hvor som helst i verden, og fortsatt få tilgang til en enhet på andre siden av kloden, gjennom smart navigering gjennom datanettverk og internett.

Kjente Hackere

Kevin Mitnick, Adrian Lamo og Michael Calce er tre kjente hackere som på hver sin måte klarte å finne kritiske svakheter i store systemer. Som engasjerte hackere flest, utnyttet de disse svakhetene for å se hvor langt inn i systemene de klarte å trenge seg.

Kevin Mitnick er et kontroversielt navn, ettersom hans hensikter aldri var å utnytte informasjonen han hacket seg til. I et intervju med Fox 5 New York sa han «*I did it for the intellectual curitosity, the pursuit of knowledge and the seduction of adventure. […] I wanted access to the source code, so I could study the source code and learn how it worked. »*[4] Mitnick ville ikke annet enn å bevise at det var mulig å hacke seg inn i store organisasjoner. For han var selve informasjonen som lå der uviktig. Han er kjent for å ha brutt seg inn i både

[4] Interview: Former hacker Kevin Mitnick. Url: https://www.youtube.com/watch?v=oadw4y4zSI4

North American Aerospace Defence Command (NORAD) i 1982, og Digital Equipment Corporation's (DEC) i 1989. Han hevder også selv at han hacket seg inn i enkelte FBI-ansatte sine telefoner for å spore deres bevegelser. På grunn av alt dette omtales han fortsatt som verdens mest kjente hacker. Han ble dømt til over 4 år i fengsel, noe mange av hans beundrere mener var en for hard straff, ettersom han aldri solgte videre noe av informasjonen han stjal.

Adrian Lamo er kjent for å ta ting for langt. I 2002 hacket han seg inn i New York Times sitt intranett, og la seg selv til i listen over ekspertkilder. Han fortsatte så med å drive forskning på flere høyt profilerte offentlige figurer. Dette ga han en straff på to års prøvetid, 6 måneder hjemfangst og en regning på 65 000 dollar for skadene han hadde påført selskapene. Til tross for dette, var han også mannen som rapporterte Chelsea Manning til politiet for lekkingen av hundre tusenvis av sensitive statlige dokumenter. Lamo hevdet selv at han var diagnostisert med Asbergers syndrom, slik som mange av de mest drevne i dataverdenen hadde. Dette forklarer deler av hans besettelse med hacking og datasystemer.

Michael Calce oppdaget store svakheter i flere store korporasjoners nettsider. Ved hjelp av ressurser han hentet fra universitetsdatamaskiner, hacket han på egenhånd Yahoo, Dell, eBay, Amazon og CNN gjennom tjenestenektangrep. Angrepene hans viste svakheter i selv de sterkeste og dyreste nettsidene, noe som reiste spørsmålet om hvorvidt informasjon og data på internett faktisk var trygge. Dette førte til at regjeringer måtte revurdere den generelle sikkerheten på nettsider, og gjøre det til en øvre prioritet. De kunne ikke risikere at mer ondsinnede hackere fikk sjansen til å gjøre det samme som Calce.

Hvordan selv unngå skadelig programvare

Til tross for at det er lett å bli utsatt for hacking, ønsker man ikke å frastå fra å bruke enhetene sine, og koble dem opp på nettet. Derfor er det viktig å forstå hvilke metoder hackere bruker for å nå din enhet, og ta forhåndsregler derfra. Det finnes utallige forskjellige måter å lure brukere på, og hackerne blir ikke annet enn smartere for hver dag som går. Roten til de aller fleste av problemene som oppstår når det kommer til hacking har å gjøre med to viktige faktorer: Tilkobling til internett og nedlastning av filer. Man kan ikke bli lurt av noen over internett dersom man ikke er koblet til internett, og man kan heller ikke laste ned uønsket programvare dersom man aldri laster ned noe programvare. Til tross for dette er det få som er villige til å ofre både internett og de mange nyttige programmene man kan finne der.

Internett og Phishing

Internett kan være både trygt og risikabelt, alt ettersom hvorvidt man tar forhåndsregler, og vet hvilke linker man skal unngå å trykke seg inn på. Hvis man deler e-postadressen sin flere steder på nettet, gjerne ved å melde seg på konkurranser, nyhetsbrev, eller annen falsk reklame, er sannsynligheten stor for at man har vært borti søppelpost. Søppelpost omtaler all uønsket e-post man mottar. E-postadressen din selges videre til personer eller firmaer som er ute etter oppmerksomheten din. Som oftest blir disse e-postene fanget opp i et «søppeøpostfilter», og når derfor aldri innboksen din. Til tross for dette klarer ikke søppelpostfilteret å fange opp absolutt all søppelpost. Hackere er kjente for å utnytte «Phishing», som er en form for digital snoking etter sensitiv informasjon gjennom e-poster. Slike e-poster kan ta mange former. Blant de farligste er de som er maskerte til å se ut som om de kommer fra banken. De har kopiert stilen til banken din, og til og med skjult avsenders e-postadresse, slik at det skal se så ekte ut som mulig. Herfra kan de lure deg til å tro at det har oppstått et problem, og trenger derfor at du sender dem innloggingsinformasjonen din. Ellers kan de også lure deg til å laste ned skadelig programvare. Man burde derfor være forsiktig med hvor man deler e-postadressen sin, og tenke gjennom hvorvidt man kan stole på de som sender e-poster. Dersom noen hacker seg inn på en brukers e-postadresse, kan han sende ondsinnede e-poster til brukerens kontakter, slik at mottakerne tar for gitt at det ikke egentlig var brukeren som sendte e-postene. Noen klare tegn på at en e-post er falsk, kan være at det finnes gjennomgående skrivefeil i e-posten eller at e-posten er sendt til flere andre e-postadresser, til tross for at den virker personlig. Man kan også se på avsenders e-postadresse og eventuelle linker i e-posten. Hvis linkene fører til et annet domene enn det avsender hevder at det skal føre til, bør det heve en mistanke. Mange går i fella hvor de tror at en avsender eller en link er til å stole på. Som bruker av internett må man være opplyst og kritisk. Tenk og vurder sikkerhet først, før du klikker inn på linker man er usikker på.

Kjente virusvarianter

Tre av de mest skadelige virusene noensinne ble nemlig spredd via e-post. Den første ble kalt «CryptoLocker», og var et typisk løsepengevirus. Den krypterte brukeres filer, og sendte en dekrypteringsnøkkel i bytte mot en sum som kunne være så dyr som 10 000 norske kroner. I Juni 2014 ble lederen for gjengen bak «CryptoLocker» tatt. Da hadde allerede en halv million mennesker blitt rammet av dette viruset. «ILOVEYOU» var et annet virus som i 2000 ble regnet som den mest skadelige noensinne. Viruset ble spredt via en e-post med tittel «I love you.» Vedlagt var en fil kalt «LOVE-LETTER-FOR-YOU.TXT.vbs». Nysgjerrige brukere lastet ned filen, uvitende om at den overskrev alle filer som fantes på enheten. Den siste typen

virus jeg skal ta for meg ble kalt for «MyDoom.» Som navnet indikerer, var ikke dette et hyggelig virus. Viruset regnes fortsatt som verdens raskest spredte e-postbaserte orm. Viruset angrep enheter med et tjenestenektangrep som spammet søppelpost fra infiserte enheter. Dette førte til økt trafikk som krasjet flere servere Det klarte å ramme selv store selskaper som Microsoft og Google. I 2004 var det estimert at over 16% av alle e-poster var infisert av MyDoom.

Offentlig internett

Man skal være forsiktig med hvilke offentlige «Wi-Fi-hotspots» man kobler seg til. Det er ikke alltid garantert at et offentlig tilkoblingspunkt er sikret, som kan gjøre en enhet mer utsatt. En av de største farene er hackernes mulighet til å plassere enheten sin mellom brukerens enhet og tilkoblingspunktet, slik at han kan hente opp all informasjonen man ellers skulle trodd reiste rett til tilkoblingspunktet. Det er derfor det også er viktig å opprette et langt og sikkert passord på sine egne rutere. Dette passordet burde ikke deles med andre enn personer man selv føler man kan stole på. Ellers kan hackere sette opp en egen «Evil Twin», som er maskert til å se ut som en beskyttet offentlig Wi-Fi-hotspot, men som egentlig er falsk. Forhåndsregler man kan ta for å sikre seg mot dette er å koble seg til offentlig internett bare ved absolutt behov. Det anbefales også å anskaffe seg en «VPN», et virtuelt privat datanettverk, som krypterer forbindelser gjennom internett, og gjør det vanskelig for hackere å få tilgang til enheter.

Sikkerhetskopiering

Hvis skaden allerede er gjort, og man ønsker å fikse en rammet enhet, finnes det måter å gjøre dette på. Store selskaper danner seg en «Information Technology Disaster Recovery Plan» (IT DRP), som skal hjelpe virksomheten i gang igjen etter en potensiell katastrofe. De har forberedt tilgjengelige servere, enheter og annen sikkerhetskopiering, for å minske nedetiden og potensielle økonomiske tap det kan medføre. Som bruker kan deler av en slik plan gi inspirasjon til hva en selv skal gjøre for å gjenopprette både enheten sin, og filene på den. Uansett hvilke filer som måtte befinne seg på enheten fra før av, er det svært lurt å sikkerhetskopiere dem. Dette kan gjøres på forskjellige måter, som alle har sine fordeler og risikoer. Man kan sikkerhetskopiere over på en fysisk enhet, som en USB-pinne, en ekstern harddisk, et minnekort eller en annen datamaskin. Dette er trygt, for fysiske enheter som ikke er koblet til noe nettverk, vil ikke selv kunne bli hacket. Risikoene ved å lagre sikkerhetskopier på en fysisk enhet, er at dersom noen skulle få tak i dem, ved for eksempel tyveri, vil det være enkelt å få tilgang til filene på den. Dette er filer som ofte kan være

personlige eller sensitive. En funksjon som mange flyttbare enheter har er at de kan krypteres, slik at de blir beskyttet av et passord. I tilfellet hvor den da skulle bli stjålet, vil ikke filene på den ende opp i feil hender. En annen metode å lagre sikkerhetskopier på, er via en nettsky. Man kan betale for å låne lagringsplass på forskjellige servere som tilbyr skylagring over internett. Blant annet utnytter Apple «iCloud», slik at filene krypteres og holdes trygge på deres servere. Dersom det skulle skje noe med den opprinnelige enheten, vil det ikke gå utover filene på den. Smarte sider ved skylagring er at man slipper å tenke på å miste eller skade en fysisk enhet. Det tilbyr gjerne også mye lagringsplass for en liten sum hver måned. Til tross for dette, har selv store selskaper opplevet at hackere har klart å få tilgang til lagringsplassen til enkelte brukere av skyfunksjonen deres. Det er derfor lurt å være oppmerksom på hvilken skyfunksjon man bruker, og at den kanskje ikke alltid klarer å levere en garantert sikkerhet.

Passord og autentisering

I tillegg til sikkerhetskopiering av filene på enhetene sine, er det også viktig å opprette passordbeskyttelse for selve enhetene. De fleste smarttelefoner har funksjoner som sperrer tilgangen til enheten, og eventuelt sletter data fra den dersom feil passord har blitt skrevet inn flere ganger. Passord skal holdes personlig, og burde huskes. Hvis brukere skriver det ned, eller forteller det videre, kan uvedkommende potensielt fange det opp, og ta nytte av det. Det anbefales å ikke bruke samme passord to steder, spesielt på bank-kontoer. Hvis et passord skulle havne i feil hender, vil uvedkommende ikke få tilgang til flere andre sensitive tjenester som bruker samme passord. En vanlig metode for hackere å knekke passord er ved et «Brute-Force» angrep, som ved hjelp av en kraftig datamaskin, kan teste tusenvis av passordkombinasjoner per sekund. Tiden det tar å finne ut et passord øker da eksponentielt basert på antall tegn, tegntyper og uforutsigbarheter i passordet. Et passord på 7 tilfeldige tegn kan potensielt knekkes på om lag en time i 2018. Dersom vi så bare legger til ett tegn, vil tiden øke til over 50 timer.[5] Nylig har biometriske autentiseringsmetoder som ansikts- og iris-gjenkjenning og fingeravtrykk blitt en populær funksjon på enheter. Disse typene autentiseringer blir bedre for hver dag som går, men er enda ikke perfekte. Hvis man derfor har tilstrekkelig med ressurser, kan en biometrisk autentiseringsmetode potensielt lures eller forfalskes.

[5] Resultater fra https://www.betterbuys.com/estimating-password-cracking-times/

Antivirus og brannmur

Antivirus, er, som navnet foreslår en type programvare som skal detektere og fjerne virus på en enhet. De fleste nye Antivirusprogrammene har også støttefunksjoner som søker etter andre typer skadelig programvare, blant annet rootkits, trojanske hester og spionvare. Programvaren har gjerne to metoder for oppdagelse av virus. Den første metoden undersøker filsystemet på en enhet, og leter etter skadelig programvare. Dersom en ny type skadelig programvare befinner seg på enheten, og antivirusprogrammet ikke har oppdatert databasene sine med informasjon om den, vil den heller ikke kunne detektere den. Av den grunn finnes det en til metode, som kjører i bakgrunnen for å detektere mistenkelig oppførsel fra programmer. Dersom programmet finner en skadelig fil, vil den som regel gi tre handlingsmuligheter: rensing, karantene og sletting. Dersom man velger rensing, vil antivirusprogrammet forsøke å fjerne bare den delen av filen som er skadelig, men fortsatt beholde selve programvaren i etterkant. Rensing kan være nyttig hvis den skadelige programvaren har spredd seg til filer man ønsker å beholde. Den svikter uansett ved rensing av for eksempel trojanske hester eller ormer, nettopp fordi det ikke finnes noen deler av filen å rense, ettersom hele filen er skadelig. Karantene vil isolere viruset til et trygt område, som behandles av antivirusprogrammet. Det vil verken fjerne eller helbrede filområdet, men isolasjonen som kommer av karantene vil forhindre spredning, og annen mistenkelig aktivitet. Sletting sletter hele filen fra filsystemet, som er nyttigst når man egentlig ikke trenger filen lenger. Hvis en skadelig programvare har spredd seg til en systemfil, kan antivirusprogrammet potensielt slette denne filen, som kan gå negativt utover enhetens generelle funksjoner. Som tidligere nevnt, er sletting best for trojanske hester og ormer. Vanligvis vil antivirusprogrammene selv anbefale en av de tre handlingene per skadelig programvare den finner. Dersom man ønsker å velge handlinger for hver skadelig programvare selv, for å være sikker på at noe ikke går galt, vil det være lurest å velge de handlingene som virusprogrammer anbefaler. To funksjoner som antivirus også gjerne tilbyr er brannmur og en aktiv beskyttelse av nettlesere. Aktiv beskyttelse av nettlesere, beskytter i sanntid mens brukere surfer internett. Den vil sjekke om domener kan stoles på, og blokkerer eller advarer om nettsider som har vært kjente for å kunne inneholde farlige filer. Man får gjerne også en beskjed før man klikker inn på dem, hvis man til tross for advarselen ønsker det. Brannmur er en beskyttelsesmetode som beskytter all nettverkstrafikk til og fra en enhet. Den leter etter uønsket kommunikasjon mellom enheter. Brannmurer jobber ved hjelp av protokoller og sikkerhetsstandarder. Den skaper en barriere mellom det klarerte interne nettverket og det uklarerte eksterne nettverket, for eksempel internett. Denne barrieren sjekker

om det eksterne nettverket selv følger protokollene den skal følge. Ikke før den gjør det, innvilges tilgang til å kommunisere med det interne nettverket, altså brukeren.

Betalt eller gratis antivirus

Det finnes mange forskjellige kommersielle antivirusprogrammer, som alle hevder å være best. Microsoft tilbyr et eget gratisprogram for enheter som kjører sitt operativsystem, nemlig «Microsoft Defender». Apple tilbyr også sin egen måte å beskytte enheter på. Flere nyere mobiltelefoner har også innebygget antivirus. For eksempel har Apple bygget mobiloperativsystemet «iOS» for sine smarttelefoner. De hevder at iOS er bygget med hovedfokus på sikkerhet, og trenger derfor ingen antivirusprogrammer. Til tross for at mange enheter har innebygget antivirusprogrammer, kan det være lurt å sjekke om enheten din likevel trenger et tilleggsprogram. Før man begynner å lete etter dette på internett, kan det være lurt å se hvilke tilbud sin egen internettleverandør har. Ofte har internettleverandører avtaler med selskaper som driver antivirusprogrammer. De tilbyr gjerne en eller flere produktkoder gratis eller til nedsatt pris. Et tredje alternativ er å finne et tredjeparts antivirusprogram på internett. Her finnes det både alternativer som er både gratis og koster penger. Som regel tilbyr de betalte virusprogrammene beskyttelse på flere nivåer enn de som er gratis. En gratisversjon inneholder som regel generell beskyttelse mot skadelig programvare. Mange kan også søke etter sikkerhetssvakheter på nettverket som enheten er koblet opp mot. De betalte abonnementene kan i tillegg tilby avanserte brannmurer, et spamfilter til brukerens e-postadresse, og blokkering av falske nettsider. Dersom man mener den ekstra beskyttelsen som følger med betalte abonnementer kan være gunstig for en selv som bruker, skal jeg ikke fraråde brukeren å ta i bruk dette tilbudet. Hvis man er usikker på hva man skal velge, vil et gratis program være godt nok for den gjennomsnittlige brukeren. Hvis man dessuten eier en liten bedrift, anbefales det å velge en betalt løsning. Dette kan være lurt for å forhindre at en skadet enhet sprer skaden til hele bedriftens nettverk, noe som potensielt kan koste bedriften dyrt. Som foreldre kan det også vært lurt å vurdere det betalte alternativet. Det vil samtidig sikre barnas aktiviteter på nettet, og lære dem om farene ved for eksempel Phishing. Uansett hvilket antivirus man skulle ende opp med, er det alltid lurt å holde den oppdatert. Biblioteket over kjente skadelige programvarer oppdateres kontinuerlig, og hackere finner nye og smartere metoder til å unngå antivirusprogrammets søkelys. Et oppdatert antivirusprogram vil alltid fungere bedre enn et som ikke er oppdatert.

Avslutning

Nå har vi blitt kjent med forskjellige typer skadelig programvare, hvem som sprer og utnytter dem, og hvordan man selv skal kunne sikre seg mot dem. Om en programvare er en variant av virus, trojansk hest eller orm, vil vi nå vite hvordan de virker og hvilke tiltak som må gjøres for å unngå, og eventuelt fjerne dem. Vi har også dannet oss et lite spekter av skadene en hacker alene klarer å utrette, og sett på eksempler fra virkeligheten. Internett er et stort marked for hackere. Det skaper en direkte tilkobling mellom brukere og hackere, selv over landegrenser. Metoder som phishing og falsk reklame er bare to av de mange tusen forskjellige metoder hackere kan bruke for å tre seg inn på enheter. Nyere metoder blir vanskeligere å oppfatte, og de utvikles daglig. Det er derfor viktig å sikre alle enhetene sine, og de viktige filene som måtte finnes på dem. Det gjøres i forkant ved sikkerhetskopiering, passordlåser og annen kryptering. Det er også viktig å holde operativsystemer, antivirusprogrammer og andre programmer oppdaterte til den nyeste tilgjengelige versjonen. Slik blir det vanskelig for hackere å utnytte svakheter i programmene. Det er nemlig umulig å nedkjempe hackere en gang for alle. Hackere og selskaper jobber mot hverandre i en evig jakt som katt og mus. Dersom et program har en sårbarhet, vil en hacker kunne finne den, og utnytte den. Samtidig som sikkerhetsprotokoller blir strammere, blir også hackere smartere. Som privat bruker er det derfor alltid lurt å ta egne tiltak, og prioritere sikkerhet for å holde enhetene sine så trygge som mulig.

Bibliografi:

(Alle linker testet: 2 November 2018)

Forsidebilde hentet fra Url:

https://www.lifewire.com/what-is-antivirus-software-152947

Betydningdefinisjoner, div. bidragsytere. Url:

http://www.betydning-definisjoner.com/Skadelig%20programvare

Wikipedia contributors. (24 Oktober 2018). Fork bomb. Url:

https://en.wikipedia.org/wiki/Fork_bomb

Wikipedia contributors. (11 November 2018). Tjenestenektangrep Url:

https://no.wikipedia.org/wiki/Tjenestenektangrep

John McCray, Junior .Net Developer. (3. August 2016). What are some of the smallest but effective computer viruses? Url:

https://www.quora.com/What-are-some-of-the-smallest-but-effective-computer-viruses

Tone Tønjum (UiO). (29. Mai 2018). virus. Url:

https://sml.snl.no/virus

Henrik Dvergsdal (Nord). (1. Desember 2016). hacker. Url:

https://snl.no/hacker

Wikipedia contributors. (26 Oktober 2018). Trojan horse (computing). Url:

https://en.wikipedia.org/wiki/Trojan_horse_(computing)

Wikipedia contributors. (24 Oktober 2018). Ransomware. Url:

https://en.wikipedia.org/wiki/Ransomware

Wikipedia contributors. (24 September 2017). Keylogger. Url:

https://no.wikipedia.org/wiki/Keylogger

NOVA PBS Official. (15 September 2014). The Secret Lives of Hackers. Url:

https://www.youtube.com/watch?v=DKzi5CYNFAg

Chris Pirillo. (10 April 2012). Who Makes Malware – and Why? Url:

https://youtu.be/GFjcM4tBjOc

Ed Tittel and Kari Finn. (5 September 2017). How to detect and remove a rootkit in Windows 10. Url:

https://www.csoonline.com/article/3222066/malware/how-to-detect-and-remove-a-rootkit-in-windows-10.html

Cybint News, Popular Posts. (16 Mars 2018). 12 Alarming Cyber Security Facts and Stats. Url:

https://www.cybintsolutions.com/cyber-security-facts-stats/

Bert Rankin. (5. April 2018). A Brief History of Malware – Its Evolution and Impact. Url:

https://www.lastline.com/blog/history-of-malware-its-evolution-and-impact/

Wikipedia contributors. (9. Mars 2016). Cracker. Url:

https://no.wikipedia.org/wiki/Cracker

Kaspersky Lab. (2018). Top Ten Most Notorious (Infamous) Hackers of All Time. Url:

https://usa.kaspersky.com/resource-center/threats/top-ten-greatest-hackers

Wikipedia contributors. (22 Oktober 2018). Kevin Mitnick. Url:

https://en.wikipedia.org/wiki/Kevin_Mitnick

Wikipedia contributors. (20. September 2018) Adrian Lamo. Url:

https://en.wikipedia.org/wiki/Adrian_Lamo

Wikipedia contributors. (30. Oktober 2018). Computer virus. Url:

https://en.wikipedia.org/wiki/Computer_virus

Wikipedia contributors. (14. September 2017). Søppelpost. Url:

https://no.wikipedia.org/wiki/S%C3%B8ppelpost

Wikipedia contributors. (17. Mai 2018). Phishing. Url:

https://no.wikipedia.org/wiki/Phishing

Norton_Team. (22 Februar 2016). The 8 Most Famous Computer Viruses of All Time. Url:

https://uk.norton.com/norton-blog/2016/02/the_8_most_famousco.html

Wikipedia contributors. (2. Mai 2017). Virtual private network. Url:

https://no.wikipedia.org/wiki/Virtual_private_network

Kasoersky Lab. (2018). How to Avoid Public WiFi Security Risks. Url:

https://www.kaspersky.com/resource-center/preemptive-safety/public-wifi-risks

Wikipedia contributors. (5. September 2018). Evil Twin (wireless networks). Url:

https://en.wikipedia.org/wiki/Evil_twin_(wireless_networks)

Nettvett.no (23. August 2018). Sikkerhetskopiering. Url:

https://nettvett.no/sikkerhetskopiering/

Brian Benton. (22. April 2014). 10 Tips on How to Prevent Malware From Infecting Your Computer—and Your Livelihood. Url:

https://www.autodesk.com/redshift/10-tips-on-how-to-prevent-malware-from-infecting-your-computer/

Wikipedia contributors. (2. Mars 2017). Antivirusprogram. Url:

https://no.wikipedia.org/wiki/Antivirusprogram

Mary Landesman (1. September 2018). Quarantine, Delete, or Clean: Which Is Best for a Virus? Url:

https://www.lifewire.com/clean-quarantine-or-delete-3972276

Wikipedia contributors. (20. Februar 2018). Brannmur (datateknikk). Url:

https://no.wikipedia.org/wiki/Brannmur_(datateknikk)

Henry T. Casey, Staff Writer. (14. Desember 2017). Why Apple iPhones Don't Need Antivirus Software. Url:

https://www.tomsguide.com/us/iphones-dont-need-antivirus-software,news-23111.html

John R. Quain, Contributing Writer (30. November 2016). Do You Really Need to Pay for Antivirus Software?. Url:

https://www.tomsguide.com/us/antivirus-software-pay-or-free,news-18570.html