CENTER FOR CYBERSIKKERHED

5. februar 2014

Trusselsvurdering: APT-angreb mod danske myndigheder, virksomheder og organisationer

Formålet med denne trusselsvurdering er at informere om omfanget af særligt avancerede hackerangreb, benævnt APT-angreb (Advanced Persistent Threat), rettet mod danske offentlige myndigheder, virksomheder og organisationer. Endvidere orienterer trusselsvurderingen om, hvordan angriberne opnår adgang til målenes it-systemer, og hvordan man kan forsøge at beskytte sig mod angrebne.

Hovedvurdering

Center for Cybersikkerhed i Forsvarets Efterretningstjeneste har kendskab til, at danske myndigheder tidligere har været udsat for særligt avancerede hackerangreb – såkaldte APT-angreb (Advanced Persistent Threat). Endvidere har et antal danske virksomheder, herunder virksomheder af betydelig størrelse og betydning for Danmark, været udsat for tilsvarende angreb.

Center for Cybersikkerhed vurderer, at det er meget sandsynligt, at statsstøttede hackere står bag angrebene.

Center for Cybersikkerhed vurderer, at danske myndigheder, virksomheder og organisationer fortsat vil blive udsat for APT-angreb. Samtidig vurderer Center for Cybersikkerhed, at det er sandsynligt, at flere myndigheder, virksomheder og organisationer allerede er blevet kompromitteret via APT-angreb uden at vide det.

Detaljeret redegørelse

Trusselsvurderingen indeholder en introduktion til såkaldte Advanced Persistent Threats, forkortet APT. Truslen fra APT-angreb er også rettet mod Danmark, og trusselsvurderingen indeholder et eksempel på, at et sådant angreb har ramt Danmark. Samtidigt gengiver trusselsvurderingen en række anbefalinger med sigte på at mindske risikoen fra APT-angreb.

Hvad er en APT?
En APT er et særligt avanceret, målrettet og vedholdende hackerangreb. Angriberne (APT-grupperne) får adgang til et netværk ved benytte sig af kendte sårbarheder eller hidtil ukendte sårbarheder, såkaldte zero-day-sårbarheder, i den software, som den angrebne part bruger. Endvidere bruger angriberne specialfremstillede hackerværktøjer, der gør dem i stand til at skjule sig i et kompromitteret netværk.

Center for Cybersikkerhed vurderer, at et APT-angreb forudsætter, at angriberen er tilknyttet eller sponseret af en organisation med tilstrækkelige økonomiske ressourcer, teknisk viden og konkret viden om det mål, organisationen ønsker at kompromittere. APT-angreb sker oftest med sigte på at udøve spionage, særligt industrispionage, og det er derfor meget sandsynligt, at det ofte er statssponserede aktører, der står bag. Teknikken bag APT-angreb er kendt i brede kredse og må formodes at blive mere udbredt, også blandt ikke-statssponsorerede aktører.

Modus – overordnet beskrivelse af de metoder, som hackerne benytter sig af
Et APT-angreb begynder med, at gruppen bag udfører en omfattende rekognoscering og undersøgelse af det netværk, der skal kompromitteres. Det er i denne fase, at angriberne får omfattende viden, som kan bruges til at tilpasse den malware, der skal bruges i angrebet. Det er også under rekognosceringsfasen, at angriberne gør sig begreb om, hvordan de bedst kan bruge social engineering og spear phishing.

Phishing og spear phishing
Inden for it-sikkerhed betyder begrebet phishing, at en angriber forsøger at skaffe sig information om et offer, såsom brugernavn, kodeord eller kreditkortoplysninger, ved at udgive sig for at være en legitim modtager af disse oplysninger. Phishing foregår oftest ved, at offeret modtager en e-mail og gennem social engineering manipuleres til selv at indtaste disse oplysninger. Ved spear phishing anvendes samme fremgangsmåde, men her er offeret særligt udpeget, og angrebet derfor målrettet.

Social engineering
Social engineering er en angrebsteknik, hvor offeret manipuleres til at udføre bestemte handlinger eller til at videregive klassificeret information uden selv at være klar over det. I forbindelse med it-sikkerhed bruges termen til at beskrive eksempelvis e-mails eller hjemmesider, der på overfladen ser legitime ud, men som i virkeligheden rummer malware. Social engineering kræver et vist kendskab til offeret for at være effektivt.

Efterfølgende afsendes malwaren. Denne er ofte enten vedhæftet en e-mail som en legitimt udseende fil eller indeholdt i e-mailen som et link. Når offeret klikker på den vedhæftede fil eller linket i e-mailen, bliver malwaren installeret og offerets computer dermed inficeret.

Figur 1: Grafisk fremstilling af et APT-angreb

Når APT-gruppen har fået etableret fodfæste i det kompromitterede netværk, bestræber den sig på, at dens aktiviteter ikke bliver bemærket. Et af kendetegnene ved APT-angreb er eksempelvis, at APT-gruppen forsøger at gemme sig i netværkstrafikken inden for normal kontortid. Endvidere gør angriberne brug af VPN-forbindelser, hvor de ved hjælp af legitime brugernavne og passwords får fjernadgang til et kompromitteret netværk.

Center for Cybersikkerhed er bekendt med, at angribere i en række tilfælde har skaffet sig adgang til samtlige passwords i den angrebne organisation via angreb på password-databasen i de kompromitterede netværk. Denne database downloades til servere, som angriberne kontrollerer. Her bliver de krypterede passwords brudt ved hjælp af såkaldte brute force-metoder. Når angriberne har adgang til brugernavne og passwords, kan de bevæge sig forholdsvist ubemærket og tilsyneladende legitimt rundt på det kompromitterede netværk.

Brute force
Brute force er en metode, som hackere kan bruge til at dekryptere en datanøgle, eksempelvis et password til et brugernavn. Selve metoden består i, at hackerne ved hjælp af særlige programmer eller særlig hardware forsøger at gætte sig frem til det rigtige kodeord.

Endelig vil angriberne forsøge at vedligeholde deres adgang til det ønskede netværk. Dette betyder eksempelvis, at de vil forsøge at installere yderligere malware skjult dybt i systemet på den enkelte computer, som kan vækkes til live, hvis APT-gruppens oprindelige bagdør opdages og lukkes.

Konkret eksempel på avanceret cyberangreb i Danmark
Et forholdsvis avanceret cyberangreb ramte Erhvervs- og Vækstministeriet i 2012. Det lykkedes angriberen at få indblik i infrastrukturen bag de forskellige net tilhørende ministeriet, få adgang til centrale servere og data og til net, som kunne skabe forbindelse til underliggende styrelsers net. For at stoppe og håndtere angrebet måtte Erhvervs- og Vækstministeriet lukke en række it-systemer ned, hvilket betød, at medarbejdere i departementet og en række styrelser i en periode ikke kunne bruge bl.a. e-mail og intranet. Center for Cybersikkerhed spillede en central rolle ved imødegåelsen af dette cyberangreb.

Tilsvarende avancerede målrettede angreb har siden fundet sted mod private virksomheder og organisationer i Danmark. Center for Cybersikkerhed er således bekendt med kompromittering af flere virksomheder indenfor højteknologiske sektorer.

Vurdering og perspektiver

Center for Cybersikkerhed har viden om udenlandske statslige og statsstøttede hackergrupper, som udfører APT-angreb mod Danmark. APT-grupperne henter ofte data fra it-systemer i virksomheder, der udvikler forskellige former for avanceret elektronik, telekommunikation og it-sikkerhed, samt virksomheder i medicinal-, forsvars- og luftfartsindustrien. Samtidig forsøger forskellige APT-grupper at få adgang til netværk tilhørende statslige organisationer og ikke-statslige organisationer.

Center for Cybersikkerhed vurderer, at de typer af APT-angreb, som er beskrevet i denne trusselsvurdering, vil fortsætte, og at danske myndigheder og virksomheder fortsat vil blive udsat for APT-angreb. Dette skyldes ikke mindst, at denne form for spionage er billig og meget effektiv. Samtidig er det muligt for de statslige aktører, der står bag angrebene, at benægte forbindelse hertil. Det skyldes, at det ofte er meget vanskeligt definitivt at afgøre, hvem der sidder bag tastaturet i den anden ende, og hermed at afgøre, om en stat står bag.

Samtidig vurderer Center for Cybersikkerhed, at det er meget sandsynligt, at flere virksomheder allerede er blevet kompromitteret af APT-grupper uden at vide det.

Anbefalinger

Det er Center for Cybersikkerheds erfaring, at myndigheder og virksomheder kan imødegå de fleste cyberangreb ved at implementere nogle få tekniske beskyttelsesforanstaltninger. Disse inkluderer whitelisting af applikationer, patchning af applikationer, patchning af operativsystemer, minimering af antallet af privilegerede brugere samt deaktivering af lokale administratorkonti. Disse foranstaltninger er nærmere beskrevet i vejledningen ”Cyberforsvar der virker”, der er udgivet af Center for Cybersikkerhed i samarbejde med Digitaliseringsstyrelsen. Vejledningen findes på cfcs.dk.

Disse tiltag er grundlæggende, men kan ikke alene imødegå alle angreb. Center for Cybersikkerhed anbefaler, at myndigheder og virksomheder, når de grundlæggende tiltag er på plads, indfører yderligere beskyttelsesforanstaltninger på forskellige komponenter fordelt over hele it-miljøet, for eksempel to-faktorautentifikation og segmentering af netværk. Når myndigheder og virksomheder indfører beskyttelsesforanstaltninger, anbefaler Center for Cybersikkerhed, at de altid følger en risikobaseret tilgang, der er baseret på en vurdering af vigtigheden af de informationer, de systemer og de medarbejdere, der skal beskyttes.

Især hvis virksomheden er i særlig risiko for APT-angreb, bør man desuden altid logge, overvåge og analysere it-miljøet for potentielle angreb og reagere effektivt på de angreb, som det ikke har

været muligt at forhindre. Man bør også gennemføre sikkerhedstekniske undersøgelser, der efterprøver dækningsgraden og effektiviteten af tiltagene, samt søge at afdække eventuelle øvrige svagheder i it-miljøet. Det er her, ligesom for de øvrige tiltag, af afgørende betydning, at virksomheder og myndigheder råder over de fornødne tekniske it-kompetencer.

Opbakning fra topledelsen er forudsætningen for ethvert succesfuldt it-sikkerhedsprogram. Det er topledelsens ansvar at vide, hvad det betyder for forretningen, hvis vigtige informationer stjæles eller lækkes, eller online services er utilgængelige i kortere eller længere tid. Det er også topledelsens opgave at uddelegere det daglige ansvar for at imødegå disse risici.

APT-angreb er hovedsageligt rettet mod myndigheder, virksomheder og organisationer, der ligger inde med viden, som stater er særligt interesserede i. Dette betyder også, at grupperne bag APT-angrebene vil gå endog meget langt for at få adgang til lige netop disse organisationers information.

Det er derfor væsentligt at pointere, at de ovenstående anbefalinger og tiltag ikke garanterer hundrede procents sikkerhed for at imødegå et APT-angreb – der er altid en risiko, hvis en organisations viden er interessant for angriberen. Denne risiko kan dog reduceres ved at implementere ovenstående anbefalinger.

Center for Cybersikkerheds rolle
Center for Cybersikkerhed er en sektor i Forsvarets Efterretningstjeneste og bidrager til at beskytte Danmark mod cyberangreb med fokus på den kritiske ikt-infrastruktur. Det sker bl.a. ved, at Center for Cybersikkerhed varsler om cyberangreb, og ved at centret efter nærmere vurdering bistår angrebne organisationer med at imødegå og afhjælpe angreb.

Center for Cybersikkerhed producerer jævnligt situationsbilleder og trusselsvurderinger, som viser et billede af den danske situation på cyberområdet og de cybertrusler, der er relevante for Danmark. Med udgangspunkt heri anbefaler Center for Cybersikkerhed, at den enkelte myndighed, virksomhed eller organisation vurderer, hvilket konkret trusselbillede den står over for, og herefter foretager fornøden risikoanalyse med henblik på at gennemføre relevante sikkerhedsforanstaltninger.

Situationsbilleder, trusselsvurderinger og vejledninger kan hentes på www.cfcs.dk