DM71

Network Admission Control

Lasse Birnbaum Jensen, 040380*

8. maj 2006

* gymer@imada.sdu.dk

Indhold

1 Indledning

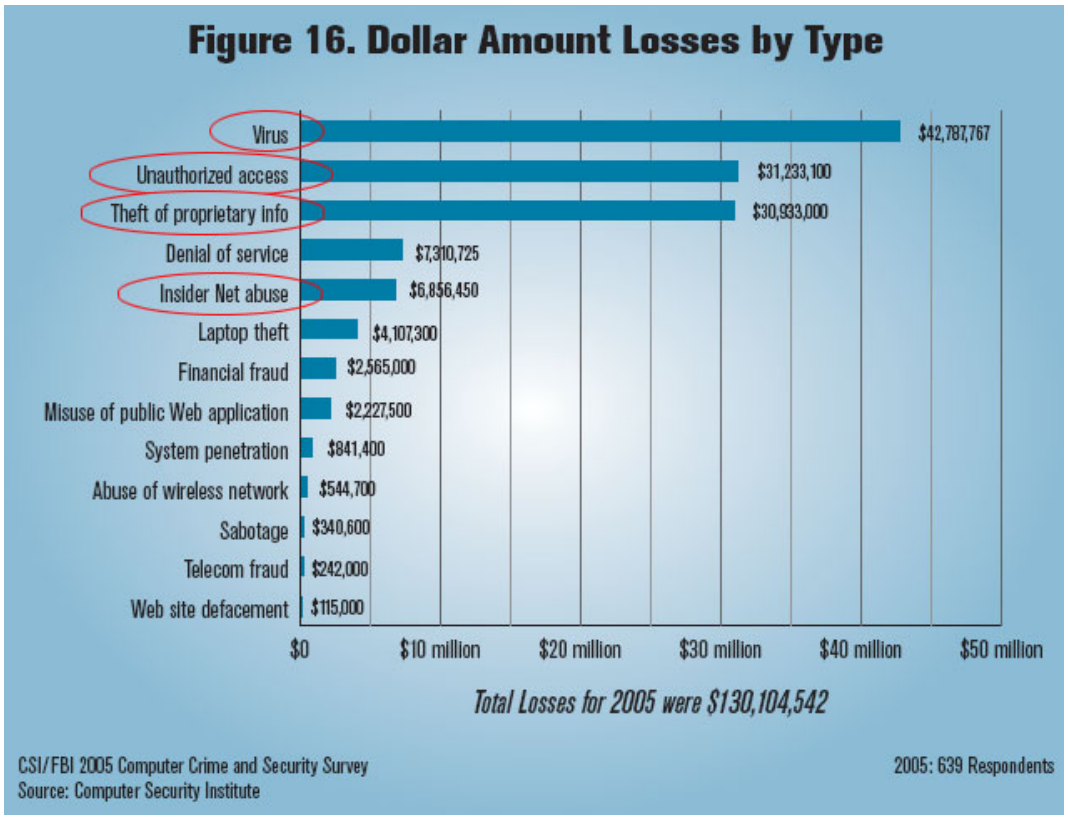
At sætte en computer på et netværk er næsten, som at spille hasard med sine dokumenter, banknøgler o.s.v. Det mest sikre ville være at alle sad med hver deres “internet”, men så er ideen ligesom væk.

Nyeste tiltag inden for trusler på netværket er ransomware, at en eller anden virus programmør tager dine data som gidsel og kræver løsepenge, for at du kan få adgang til dem igen. Derudover kan man blive franarret sit brugernavn og kodeord til netbank eller “bare” få en forstyrrende virus eller reklame på sin computer.

En måde at sikre netværket og computeren mod disse ting er; Network Admission Control (NAC). I dette dokument vil det blive gennemgået hvordan dette foregår, med udgangspunkt i produktet Cisco Clean Access, fra Cisco System.

2 Sikkerhedstrusler

Som nævnt er truslerne for computere og netværksforbundne computer store og mange. FBI har i deres årlige computer sikkerhedsrapport lavet følgende opgørelse ud fra tilbagemeldinger fra 639 amerikanske virksomheder. Tabstallene skal nok ikke tages for pålydende, da det er dem virksomhederne oplyser til forsikring,retsager m.m. Jeg mener dog søjlernes indbyrdes relative størrelse kan sammenlignes.



Figur 1: Opgørelse af tab ved incidents

Som det ses i figur 1 har jeg fremhævet 4 type med en ring. Dette er dem jeg kort vil sige lidt om i forbindelse med de følgende afsnit.

2.1 Fokus tilbageblik

De sidste par år har fokus i it-sikkerhedsverdenen været på virus.

Den først er “virus”; den nok mest kendte type af sikkerhedstrusler, og også den type de fleste privatpersoner har erfaring med. Fokus har i flere år været rettet meget på virusbekæmpelse, dette betyder at de fleste mennesker har efterhånden lært at man ikke skal åbne ukendte vedhæftede filer i mails eller blindt stole på programmer man henter på internettet. Ligesom de fleste har fundet ud, at de skal opdaterer deres styresystem, så det ikke er sårbart.

Set ud fra et erhvervsmæssigt synspunkt er virus også noget der håndteres; ved virusscanning af indkomne mail i mailsystemer og alle medarbejdere har anti-virus installeret. Ikke alle er dog lige gode til at holde deres systemer opdateret.

2.2 Fokus i fremtiden

Med virus delvist under kontrol er man begyndt, at se nye trusler mod netværk og de tilkoblede resourcer. Derfor vil fokus ændrer sig mod følgende:

“Unauthorized access”, uautoriseret adgang til netværk. Mange virksomheder har åbne netværk, hvor man bare skal koble sin computer til stikket i væggen og så er man på netværket. Dette giver adgang til f.eks. virksomhedens it-resourcer, programmer o.s.v. Eller mulighed for f.eks. at sende spam til folk, hvorved virksomheden vil se skyldig ud.

“Theft of proprietary info”, tyveri af proprietær (ikke-fri) information, det kunne være produktion-shemmeligheder, endnu ikke patenterede opfindelser o.s.v. Dette kan være en medarbejder eller en computer der er inficeret, der giver mulighed for, at informationen hentes.

Disse to typer kan være store trusler mod alle virksomheder og også private, ligeledes er den sidste “insider net abuse”, internt net misbrug, også et stigende problem, da medarbejde bruger flere af virksomhedens it-resourcer til private formål.

Specielt de først 2 nævnt i dette afsnit er i foruroligende fremgang. Dette vil man forsøge, at afhjælpe ved hjælp af network admission control.

3 Network Admission Control

NAC er en ret ny måde at tænke netværkssikkerhed på. Der tages udgangspunkt i at man ønsker at have et dynamisk og robust netværk. Inden klienter kommer på netværket skal de godkendes, hvilket giver netværk den egenskab. På den måde sikre man sig mod f.eks. at få en virusinficeret computer ind på det stort netværk, hvor den kan sende sin smitte videre.

Målene med NAC er blandt andet at:

- mindske internt misbrug af it-resourcer
- få mere dynamisk sikkerhed på netværket
- minimere omkostningerne ved sikkerhedhændelser

NAC er et framework, der kombinerer nogen af de nyeste sikkerhedsmekanismer i netværk og på de enkelte klienter. På papiret består systemet af 4 tilstande/trin:

- Godkendelse og adgangstildeling
- Scanning og evaluering
- Karantæne
- Opdatering og genindsættelse

De enkelte trin er nærmere beskrevet i afsnit 4.

3.1 Teknologierne

En rækker mere eller mindre kendte teknologier anvendes:

- DHCP
- IPsec
- 802.1x
- Sikkerhedsscanninger
- Anti-spyware
- Anti-virus
- Patch-inspektion

De fleste er kendte, DHCP - “Dynamic Host Configuration Protocol”, som sikre tildeling af ip-adresse til de tilkoblede enheder, IPsec - “Internet Protocol Security”, en suite af protokoller til kryptering og udveksling af information.

En af de nyere er 802.1x, en IEEE standard for port-baseret adgangskontrol. Dvs. inden man får adgang til switch/router porten skal man godkendes. Denne teknologi spiller en meget central rolle i NAC. Da det er her, det afgøres om en enhed gives adgang til et netværk.

Et anden vigtigt komponent er sikkerhedsscanningerne, disse er meget brugt indenfor diagnostisering af enheder og meget kan afsløres når man scanner en computer. Det kan være services der kører på computeren eller installerede bagdøre på systemet.

De 3 sidste er velkendte af de fleste computer brugere. Dog er den sidste “patch-inspektion” er dog blevet automatiseret, således man ikke manuelt skal finde ud af hvilket opdateringer man har eller ikke har installeret.

4 Cisco Clean Access

Cisco Clean Access (CCA) er en implementation af NAC frameworket af Cisco Systems. Det er først del af deres "Cisco Self-Defending Network Initiative", som i fremtiden vil indeholde deres netværkssikkerheds produkter.

CCA består af 3 centrale komponenter:

- Clean Access Server (CAS)
- Clean Access Manager (CAM)
- Clean Access Agent (CAA)

CAS er den server der håndterer sikkerhedsscanning og evaluering i henhold til de regler, som er konfigureret i CAM serveren. CAS sørger også for godkendelse af password med mere. CAS er lavet således, at brugernavn og password kan tjekkes mod mange forskellige tjenester. F.eks. understøttes integration med Microsoft Active Directory, Kerberos, LDAP og flere. Dette gøre det nemmere for en virksomhed at integere CCA i deres nuværende netværk.

CAA sørger for at kommunikere f.eks. anti-virus versioner til CAS, som behandler dette og sender svar retur. CAA er desuden også 802.1x klient.

4.1 Samarbejdspartnere

En af de afgjorte styrker ved CCA er Cisco store arbejde med at få andre leverandører af it-sikkerhedssoftware med i systemet. Lige for at nævne et par eksempler er der indgået aftale med:

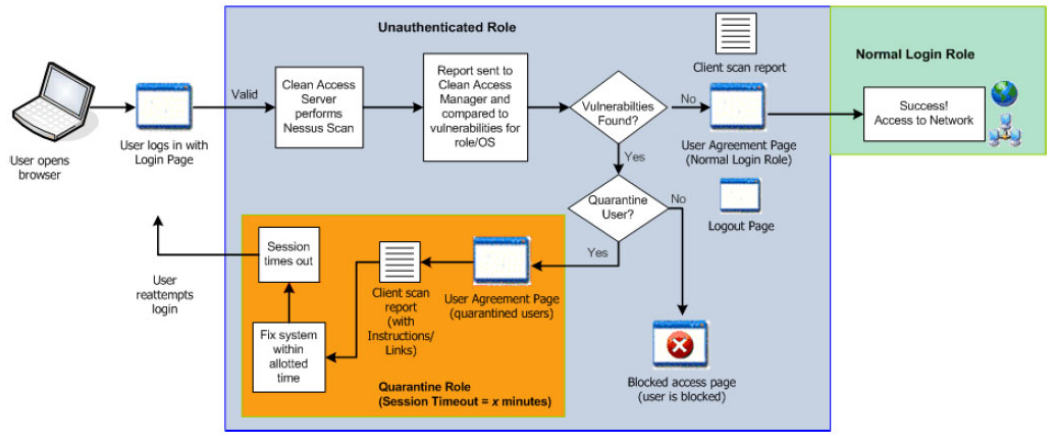
- Sophos (anti-virus)
- Symantec (anti-virus, firewall m.m.)
- Ad-aware (anti-spyware)

4.2 Eksempler på CCA i drift

2 eksempler vil blive gennemgået. Det første er CCA uden agent installeret på computeren der kobles på netværket, det andet med agent installeret.

4.2.1 CCA uden agent

Uden agenten betyder det, at brugernavn og password ikke kan sendes via 802.1x, og derfor afkræves der brugernavn og password på en hjemmeside.



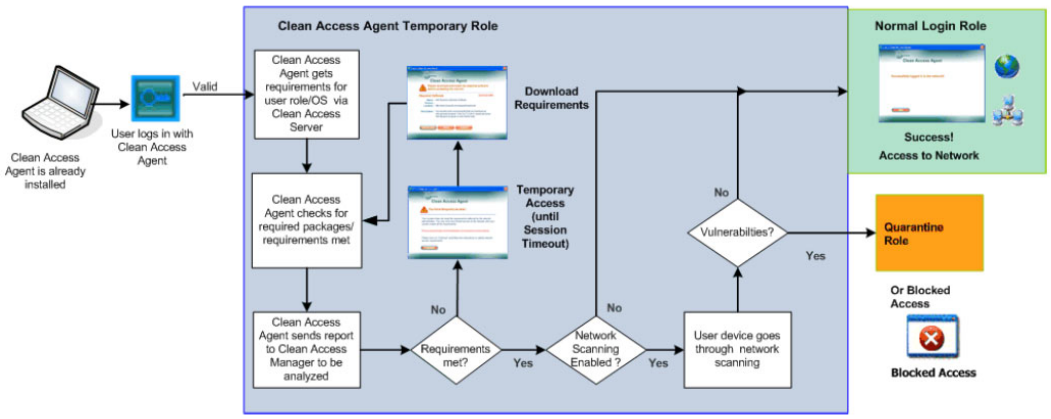
Figur 2: CCA uden agent

Efter brugernavn og password er modtaget scannes computeren af CAS og der tjekkes for kendte sikkerhedsfejl på computeren. Hvis computeren lever op til alle krav gives adgang til netværket.

Hvis computeren ikke lever op til sikkerhedspolitikken så er der 2 muligheder for den videre process. Hvis der ikke er karantæne muligheder så bliver computeren blokeret. Alternativt sendes computeren til karantæne zonen hvor brugeren kan f.eks. finde opdateringer til systemet eller kontakte helpdesken i virksomheden.

4.2.2 CCA med agent

Hvis CAA er installeret på computeren giver den en anden situation, da agenten vil sende brugernavn og password. Dvs. at for brugeren vil denne process være transparent. Via agenten kan CAS tjekke at f.eks. de korrekte/krævede Windows opdateringer er tilstede.



Figur 3: CCA med agent

Når ovenstående er tjekket sendes videre til enten en zone, hvor evt. manglede opdateringer installeres automatisk af agenten. Hvis alt er ok udføres en scanning af computer, hvor resultatet afgører, om der gives adgang til netværket eller computeren sendes i karantæne zonen.

4.3 Fordele

At lave et sikkerhedssystem som NAC omkring ens netværk giver en række fordele.

4.3.1 Sikre overholdese af sikkerhedpolitikker

Ved at have et system hvor en computer først skal registreres, scannes og evalueres sikre, at sikkerhedpolitikkerne hos virksomheden overholdes. Virksomheden kan derfor afgøre hvem og hvilke krav der stilles til f.eks. gæster på netværket.

4.3.2 Seperation af afdelinger og grupper

Med 802.1x og en dynamiske tildeling af netværksadgang kan netværket deles op i VLANs, udfra ens credentials og ikke efter hvilket lokale man er i. Derved kan en medarbejder i afdeling X, sidde i afdeling Y og kun have adgang til de ting han i følge hans credentials skal have. Dvs. han ikke har adgang til afdeling Ys resourcer, blot fordi han sidder i den.

4.3.3 Centralt styret

Fra centralt hold kan man vedligeholde de krav der stilles. Dvs. man ikke skal rundt i alle afdeling og f.eks. lave installationer på alle maskiner for at sikre de lever op til sikkerhedpolitikerne.

4.3.4 Karantæne zone

Endnu en kæmpe fordel er karantæne systemet. Ved at have dette kan man sørge for at holde problemerne i kontrollerede zoner. Her kan problemer med computerne udredes inden de kobles på det rigtige netværk.

4.3.5 Bedre netværkssikkerhed

Alle ovenstående løfter bund niveauet for sikkerheden og derved samlet set sikre, at virksomheden står stærkere it-sikkerhedsmæssigt.

4.4 Ulemper

Der er også udlemper ved så store ændring og krav til netværket.

4.4.1 Leverandør afhængigt

At være bundet til en bestemt leverandør er som regel ikke noget virksomheder er meget for. Men ved at vælge NAC binder man sig 100% til Cisco, da NAC kræver at alt netværksudstyr er fra Cisco. Hvis man i fremtiden vil have en mere sikker løsning, hvis der kommer en sådan, som ikke er fra Cisco skal alt udstyr højst sandsynligt udskiftes.

4.4.2 Dyr løsning

Da det er leverandør afhængigt, så kan man ikke gå ud og finde billigere alternative leverandører til dele af netværket. Det vil derfor være en relativt dyr løsning, da f.eks. Cisco er en del dyrere pr. netværksport end de fleste af deres konkurrenter.

4.4.3 Styring

Som alle andre systemer kræver det en erfaren administrator eller gruppe af administratorer. Hvis man laver en fejl i systemet vil det resultere i at alle virksomhedens afdelinger vil blive berørt.

4.4.4 Delvist klient baseret

Endnu et kritik punkt er at systemet er delvist klient baseret, da Clean Access Agent, helst skal være installeret på alle klienter. I det man lader klienterne tjekke sig selv, kan man også forestille sig, at disse tjeks kan slås fra eller endnu værre, man kan sende falske resultater til netværket, CAS serveren.

4.4.5 Stadig under udvikling

Da systemet stadig er under udvikling er der fejl.. og der er stadig kun et begrænset antal routere/switche der understøtter CCA 100 %.

4.5 Fremtiden

Cisco har planer for NACs fremtid, denne involverer blandt andet:

4.5.1 Trafik analyse

Mulighed for at kunne analysere trafikken på netværket for at finde uregelmæssigheder. Dette er et fornuftigt tiltag, men kan omgås ved at “træne” klienterne langsomt. Derved vil NAC ikke se f.eks. en stor stigning i trafik, men en langsom stigning over lang tid. Denne vil blive betragtet som en naturlig udvikling af trafikken.

4.5.2 Bedre understøttelse

Da systemet er under udvikling så vil der komme bedre understøttelse til flere operativ systemer for agenten og flere Cisco enheder vil understøtte CCA.

4.5.3 Flere samarbejdspartnere

Cisco arbejder hele tiden på at få flere med i projektet. Jo flere de får med jo bredere platform vil de stå med på markedet og kunder vil ikke skulle skifte f.eks. anti-virus leverandør for, at implementere CCA på deres netværk.

5 Konklusion

Et system som CCA har klart sine fordele, men også udlemper. Jeg mener, at virksomheder der anvender denne teknologi vil få meget ud af løsningen, men det vil være meget stor investering selv for en stor virksomhed.

Denne nye måde, at tænke netværkssikkerhed finder jeg meget interessant, og mon ikke der kommer andre og måske bedre forslag til løsninger i fremtiden.

Specielt at sikkerheden/begrænsningerne følger med en person uanset hvor vedkomne måtte koble sig på, finder jeg meget spændende. Dette har helt sikkert store fremtidsudsigter.

SDU har f.eks. planer om at anvende 802.1x på alle netstik i undervisningslokaler. Derved kan man opnå at brugeren skal afgive credentials og samtidig sikre at brugeren ikke f.eks. har adgang til et fakultets it-resourcer, med mindre vedkomne er tilknyttet dette. Der er dog ikke tale om at implementere NAC på netværket, kun det ene komponent.

Lasse Birnbaum Jensen