VAASAN AMMATTIKORKEAKOULU
VASA YRKESHÖGSKOLA
UNIVERSITY OF APPLIED SCIENCES

Mimosa Kjellman

ÖVERBELASTNINGSATTACKER MOT NÄTVERK OCH HUR MAN SKYDDAR SIG MOT DEM

Case Anvia ICT

Informationsbehandling
2013

VASA YRKESHÖGSKOLA
Informationsbehandling

ABSTRAKT

Författare	Mimosa Kjellman
Lärdomsprovets titel	Överbelastningsattacker
År	2013
Språk	svenska
Sidantal	47 + 1 bilaga
Handledare	Erik Wahlman

Syftet med detta lärdomsprov är att göra en kartläggning över överbelastningsattacker mot nätverk samt hur man skyddar sig mot dessa, sett ur internetleverantörens synvinkel. Lärdomsprovet är gjort på uppdrag av Anvia ICT, Österbottens ledande internetleverantör.

DDoS-attacker är ett ständigt växande hot mot dagens IT-samhälle och ur en internetleverantörs synvinkel är detta ett väldigt känsligt problem. Jag kommer att berätta om datorkommunikation, olika typer av DDoS-attacker, vilka motiven bakom dessa attacker är, övriga hot mot datasäkerheten samt vad man kan göra för att skydda sig mot dem. Lärdomsprovet innehåller också en jämförelse mellan tre olika försvarssystem mot DDoS-attacker.

Avslutningsvis redogör jag för resultaten från kartläggningen samt resultaten från jämförelsen. Av resultaten framgår att utan ett försvarssytem, specifikt utvecklat för skydd mot DDoS-attacker, är det omöjligt att skydda sig mot DDoS-attacker. Resultaten från jämförelsen visar att försvarssystemen mot DDoS-attacker arbetar på samma sätt men tar hand om den skadliga trafiken på olika sätt.

Ämnesord Överbelastningsattacker, DoS, DDoS, informationssäkerhet

VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES
Informationsbehandling

ABSTRACT

Author	Mimosa Kjellman
Title	DoS-attacks and how to protect ISP from them
Year	2013
Language	Swedish
Pages	47 + 1 appendix
Name of Supervisor	Erik Wahlman

The purpose of this thesis is to conduct a survey of denial-of-service attacks against networks and how to protect yourself against these, from an ISP's point of view. This thesis is done on behalf of Anvia ICT, leading ISP in Ostrobothnia.

DDoS attacks are an ever-growing threat to today's IT community and from a internet service provider's point of view, this is a very sensitive issue. I will tell you about computer communication, different types of DDoS attacks, the motives behind these attacks, other information security threats and what you can do to protect against them. The thesis also includes a comparison between three different defense systems against DDoS attacks.

Finally, I describe the results of the survey and the results of the comparison. The results show that without a defense system against DdoS-attacks, specifically developed for protection against DDoS attacks, it is impossible to protect a network against DDoS attacks. The results of the comparison show that the defense systems against DDoS attacks work the same way but are taking care of the malicious traffic in different ways.

Keywords DoS, DDoS, information security, denial of service

INNEHÅLL

FÖRTECKNING ÖVER FIGURER OCH TABELLER

FÖRTECKNING ÖVER BILAGOR

ORD OCH UTTRYCK

Anonymous	En grupp hackers, ”hacktivist”-grupp, som ansvarar för några av de största politiskt motiverad cyberattackerna som inträffat under de senaste åren.
Botnät	En samling av datorer, som ofta kallas ”Zombies”, infekterade med skadlig kod som gör det möjligt för en angripare att styra dem.
DoS	Denial of Service. DoS-attacken riktar sig mot tillgängligheten hos en viss sida eller tjänst. Till skillnad från andra cyberattacker är DoS-attackerna primära mål inte att stjäla information utan att slöa ner eller helt ta ner en webbsida.
DDoS	Distributed Denial of Service. Attacker som går till på samma sätt som DoS-attacker men där angriparen använder sig av flera datorer för att öka attackens effektivitet och styrka.
DNS	Domain Name Server. DNS konventerar automatiskt den adress vi skriver in i vår webbläsare till IP-adressen för webbservern som skall visa denna sida.
CERT-FI	En grupp inom Kommunikationsverket vars uppgift är att ge råd och information om informationssäkerhet samt ta emot anmälningar om kränkningar av informationssäkerheten.
Flood	Samlingsnamnet för DoS-attacker där angriparen ständigt försöker skicka trafik för att översvämma den attackerade servern så ingen annan kommer åt den.

Gateway	Utrustning som kopplar samman nätverk med olika protokoll.
Hackare	En mycket datakunnig person som använder sina kunskaper för olika syften.
IDMS	Intelligent DDoS Mitigations System. Ett system som jobbar på alla OSI-modellens lager och vars uppgift är att skydda ett nätverk från DdoS-attacker.
Ping	Ping-kommandot används för att kontrollera om en annan dator i nätverket svarar. Det kan berätta en hel del information om status för nätverket och datorerna man kommunicerar med.
SSL	Secure Sockets Layer, ett protokoll som utvecklats av Netscape för överföring av privata dokument via Internet.
SYN – ACK	Synchronize – Acknowledgement. Handskakningen via TCP sker genom att avsändaren skickar ett synkroniserat paket till mottagaren. Mottagaren skickar avsändaren ett SYNchronize-ACKnowledgement-paket och avsändaren skickar mottagaren ett ACKnowledgement-paket.
VPN	Virtuellt privat nätverk, gör det möjligt att via internet ansluta en dator till ett privat nätverk.
TCP/IP	Transmission Control Protocol / Internet Protocol. Kommunikationsprotokollet för trafik på internet, definierar hur elektronik bör vara kopplade till internet samt hur data skall skickas.

TDoS	Telephony Denial of Service. Fungerar på samma sätt som vid DoS-attacker men det är telefonlinjen som översvämmas.
UDP	User Datagram Protocol, via detta protokoll sker all datahantering mellan olika datorapplikationer.
VoIP	Voice over Internet Protocol. IP-telefoni som sker via internet.

1 INLEDNING

För varje dag som går blir samhället allt mera beroende av Internet. E-handeln växer, bankerna styr sina kunder till att använda online-tjänster och även skatte-deklarationen sköts via internet. Utvecklingen av datorsamhället för med sig både nya lösningar och nya sårbarheter. Automatiserade processer förenklar utförandet av vardagliga sysslor och ärenden samtidigt som det lämnar en olåst dörr till de som har kunskapen om hur man kan manipulera dessa processer för egen vinnings skull.

I takt med att allt fler samhällsviktiga system kopplas upp till internet, ökar vårt samhälles sårbarhet mot IT-angrepp. Det är i skrivande stund inte främmande makt eller organiserad brottslighet som är största hotet mot världsfreden; "Precis som kärnkraft användes som krigsföring under den industriella tidsperioden, har internetkrigsföring blivit den strategiska krigsföringen under 2000-talet" säger USA: s försvarsminister Leon Panetta. Cyberspionage och cybersabotage är redan verklighet. Och undersökningar gjorda av Symantec gjorde det klart att alla företag, oavsett dess storlek, är potentiella måltavlor för angripare. (Symantec Corporation 2012, 14-15)

Företag är en ständig måltavla för de som försöker stjäla data eller göra företaget helt onåbar. Dessa hot är ofta en blandning av många olika attacker och är speciellt utformade för de organisationer som utgör målgruppen. Enligt CERT-FI:s översiktsrapport 2013 var de vanligaste säkerhetshoten under 2012 överbelastningsattacker, trojaner och infektioner från skadliga program. Speciellt drabbades media mot sårbarheter i program, dataintrång och utpressningsprogram. (CERT-FI 2013)

Överbelastningsattacker genererar dagligen nyhetsrubriker runt om i världen med artiklar över hur en illvillig individ eller grupp kunnat orsaka stor förödelse genom att krascha webbsidor med hjälp av överbelastningsattacker. Överbelastningsattacker ter sig märkliga även för datasäkerhetsexperter. För det första utnyttjar de inte en sårbarhet som behöver korrigeras. För det andra är datan som används under attacken legitim, endast kombinationen av mycket data blir

destruktivt. För det tredje är attackerna långa och kan vara upp till timmar eller dagar, i stället för sekunder och minuter. (Kenig, Manor, Gadot, Trauner 2012, 4-5)

Under 2000-talet har man sett att antalet överbelastningsattacker ökar stadigt från år till år. För internetleverantören är dessa attacker påfrestande. De orsakar bland annat avbrott i de tjänster internetleverantören erbjuder sina kunder vilket i sin tur leder till missnöjda kunder. Det är i dagens läge väldigt svårt och dyrt för en internetleverantör att skydda sig mot överbelastningsattacker men att inte skydda sig från överbelastningsattacker blir också dyrt i längden (Kenig m.fl. 2012, 9-11).

I detta lärdomsprov kommer jag att berätta om överbelastningsattacker. Jag behandlar hur dessa attacker ser ut och fungerar, vad deras syfte är samt vem som ligger bakom dem. Eftersom att överbelastningsattacker är ett ständigt problem och hot mot Anvias nätverk har Anvia Abp begärt offerter från tre olika leverantörer av IDMS-system. I detta lärdomsprove berättar jag om dessa företag och deras produkter samt gör en jämförelse dem sinsemellan.

1.1 Anvia Abp

Anvia Abp, före detta Vasa Läns Telefon AB, är den dominerande leverantören av nätförbindelser i Österbotten. Anvia erbjuder moderna och högklassiga lösningar inom kommunikation, dataadministration, säkerhet samt överföring av rörlig bild och ljud för konsumenter och företag. Verksamheten hos Anvia har redan från första början baserat sig på att bygga, utveckla och underhålla fasta nät. I början skedde detta främst i form av telefonnät – i dagens läge förmedlas datatrafik via snabba, fasta bredbandsnät. Anvia-koncernen består av tre affärsområden; Anvia ICT, Anvia TV och Anvia Securi. (Anvia Abp 2013)

Anvia ICT erbjuder fullständiga telekommunikations- och IT-tjänster till såväl konsumenter som företag och även till andra operatörer. Anvia TV vill vara en föregångare i synnerhet inom användarvänliga tv-produkter och tv-tjänster. Målet är både att växa och att förbättra lönsamheten.

I nästan alla sina produktgrupper är Anvia TV redan bland de största aktörerna i Finland och målet är att ytterligare förbättra positionen på marknaden inom dessa grupper. Hibox iptv-programvaror har även sålts på den internationella marknaden.

Anvia Securis mål är att vara en nationell partner för kunderna inom säkerhetslösningar. Tillväxtsatsningarna riktas i synnerhet mot elektroniska säkerhetssystem. Dessa utgör för tillfället cirka 20 % av omsättningen men uppskattas utgöra hälften av omsättningen år 2013. Ett annat växande område är tjänsteverksamheten till exempel larmcentral- och underhållstjänster. Den geografiska spridningen av Anvia Securis verksamhetsställen gör det möjligt att erbjuda mindre kunder lokal service, medan större kunder kan betjänas på regional och även nationell nivå.

1.1.1 Anvia ICT

Anvia ICT:s syfte är att vara den ledande ICT-leverantören till konsumenter och företag i Österbotten och växa även inom andra geografiska områden med säkerhetslösningar, TV-affärsverksamhet och utvalda IT-tjänster till exempel molntjänster och applikationslösningar. En förutsättning för framgång är tjänster som grundar sig på sakkunskap, kompetens och närhet.

Anvia ICT affärsidé:

”Att vara kundernas bästa samarbetspartner inom kommunikationsteknologi”

Anvia ICT värden

”Närhet till kunden och kontinuerlig utveckling”

Anvia ICT vill behålla sin starka ställning i Österbotten hos konsumenterna. Under de kommande 10 åren har Anvia ICT som mål att kunna erbjuda hela Södra Österbotten, Mellersta Österbotten och Österbotten snabba fiberförbindelser. Detta innebär att under de kommande 10 åren kommer alla kopparkablar i det nuvarande nätet att bytas ut till optofiber. För Anvia ICT innebär detta investeringar på tiotals miljoner euro och för kunden utvidgade möjligheter att dra

nytta av nätet. För att nå detta mål måste processerna för nätbyggande utvecklas och automatiseras och kostnadseffektiviteten förbättras. (Anvia Abp 2013)

Från den nuvarande oenhetliga organisationen övergår man inom Anvia Företagstjänster till en kundinriktad struktur, där man kan sköta kunderna mera helhetsbetonat och på så vis öka värdet på kundrelationen. Anvias konkurrensfördelar är sakkunskap, närhet till kunden och förmåga att i helhet kunna betjäna kunden. Försäljningen och kundbelåtenheten främjas av effektiva och kvalificerade processer för försäljningssupport och service. Företagstjänsternas utbud utvecklas mot produktifierade, i stor utsträckning automatiserade, ICT-tjänster kring vilka det är möjligt att skräddarsy kundspecifika lösningar. De fortlöpande tjänsternas andel av omsättningen ökas planenligt. (Anvia Abp 2013)

2 BAKGRUND

Kraven på dagens internetleverantörer är större än någonsin. Internetleverantörer måste bland annat kämpa mot växande DDoS-attacker, som har vuxit i storlek, frekvens och förfining under senare år. För att internetleverantören skall kunna säkerställa att deras tjänster finns tillgängliga, måste internetleverantören kunna upptäcka, analysera och minska DDoS-hot innan de utvecklas till kostsamma avbrott i tjänsternas tillgänglighet.

Det ökade behovet av snabbare hastigheter och ökad bandbredd gör att internetleverantörerna måste ha en skalbar och effektiv datasäkerhetsstrategi för att kunna förbli konkurrenskraftiga på marknaden. Att upprätthålla en konkurrensfördel på marknaden kräver också att internetleverantören kan skilja sig från sina konkurrenter. Ett av de bästa sätten att lyckas med det är att först få kunderna medvetna om DDoS- och datasäkerhetshot för att sedan kunna erbjuda kunderna kostnadseffektiva drifttjänster inom nätverkssäkerhet. (Arbor Networks Inc.. 2012, 1-5)

3 ÖVERBELASTNINGSATTACKER

3.1 Datorkommunikation

3.1.1 Bit, byte och paket

Den minsta dataatomen kallas bit. En bit består av ett värde, antingen en 0 eller 1, också känt som binärt. Bitar delas in i grupper om åtta bitar och bildar tillsammans en byte. En byte kan innehålla ett tecken, en bokstav eller ett nummer (upp till 255). Flera bytes bildar tillsammans ett paket som skickas genom nätverket.

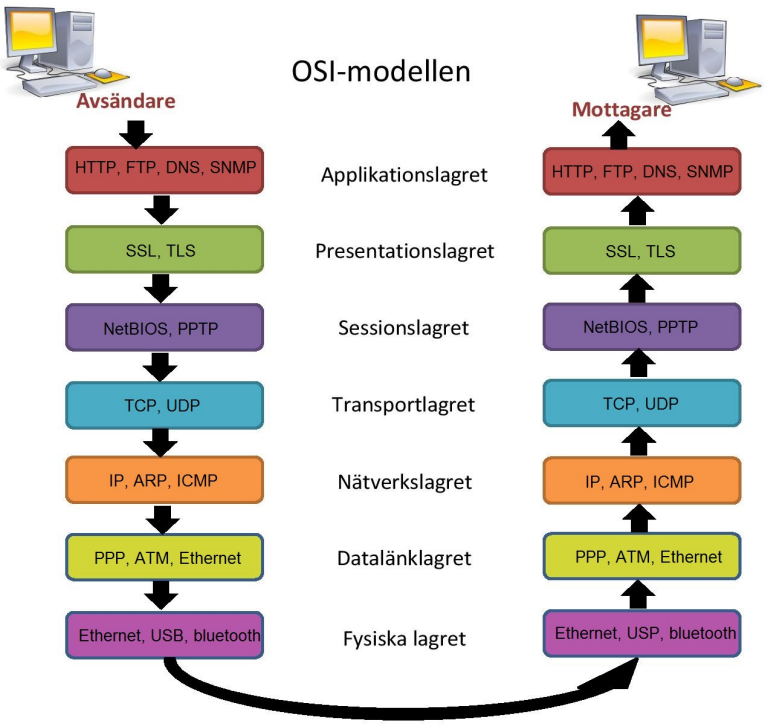
3.1.2 OSI-modellen och datorkommunikation

OSI står för Open Systems Interconnection och OSI-modellen är ett resultat av ett projekt som genomfördes under 80-talet vars uppgift var att ta fram standarder inom datorkommunikation. OSI-modellen består av 7 olika lager, och dessa lager har var för sig en egen uppgift när det kommer till datorkommunikation. Föreställ dig att du skickar ett e-post meddelande till en vän, så här går den processen till genom OSI-modellen (Cowder 2008):

7. Applikationslagret: Du använder t.ex. Microsoft Outlook och skriver ett e-postmeddelande och klickar på skicka-knappen. Då vaknar applikationslagret och kontrollerar ditt meddelande bl.a. vem är mottagare, vem är avsändare, med vilket protokoll ska meddelandet skickas. I applikationslagret används bl.a. protokollen FTP, Telnet, SMTP, HTTP.
6. Presentationslagret: Här översätts ditt meddelande från din text till ett enhetligt språk som resten av applikationslagret kan förstå. Här används SSL, MIME protokoll.
5. Sessionslagret: Ditt e-post meddelande har nu blivit data och du skulle inte längre känna igen innehållet eftersom det har översatts till, för oss människor, ett helt ologiskt språk. I det här skiktet öppnas, underhålls och stäng de anslutningar som behövs för kommunikation inom OSI-modellen med hjälp av RIP, SAP, VPN protokoll. Det här lagret meddelar åt nästa lager att det meddelande är redo för att skickas.

4. Transportlagret: Meddelandet delas upp i exakt lika stora paket innan det skickas iväg. I transportlagret används transportprotokollet TCP och UDP. TCP upprättar en anslutning mellan två datorer på nätverket via "uttag" som bestäms av IP-adress och portnummer.
3. Nätverkslagret: Här adresseras paketet och här bestäms också vilken väg paketet skall ta. Nätverkslagret är också ansvarig för att översätta nätverksadresser och namn till maskinens MAC-adress. Lagrets största uppgift är dess förmåga att kunna tillåta att två olika nätverk, med olika adress-scheman, får skicka data med varandra. Lagret tillåter också olika protokoll att kommunicera med varandra för att förstå vart paketet är på väg.
2. Datalänklagret: Paketen av ditt e-postmeddelande översätts till rådata, bitar, dvs. ettor och nollor. Hanterar kommunikationen mellan nätverkslagret och fysiska lagret. Här definieras också de metoder som används för att transportera och ta emot data.
1. Fysiska lagret: Lagrets uppgift är att etablera, upprätthålla och avsluta de fysiska anslutningarna som behövs för skickande av informationen.

När meddelandet kommer fram till mottagaren gås samma OSI-modell igenom men andra vägen, dvs. fysiska lagret på mottagarens sida tar emot e-postmeddelandet, datalänklagret översätter bitar till paket. Nätverkslagret kollar paketens adresser, dvs. din dators MAC-adress. Paketen monteras ihop i transportlagret. Sessionslagret meddelar till presentationslagret att vara redo för att ta emot meddelandet. Presentationslagret översätter meddelandet till sin ursprungliga form och applikationslagret skickar meddelandet vidare till mottagarens e-postprogram.



Figur 1. *Illustration över OSI-modellen*

3.2 Vad är en överbelastningsattack?

En överbelastningsattack är ett försök av en hacker att förhindra legitima användare av en tjänst från att använda just den tjänsten. DoS-attacker är inget nytt, de har funnits i över 20 år och utvecklas hela tiden. Under en DoS-attack används en dator och en uppkoppling för att översvämma en server med trafik med syftet att överbelasta och göra serverns resurser otillgängliga. Dessa resurser kan bestå av en specifik dator, en port, ett program eller ett helt nätverk. DoS-attacker kan också riktas mot konkreta systemresurser så som bandbredd, diskutrymme och processortid. Dessutom kan DoS-attacker utformas för att köra skadlig kod mot processorn, utnyttja sårbarheter i operativsystemet och krascha operativsystem helt och hållet. Den övergripande likheten i dessa exempel är resultatet; systemet, datorn eller tjänsten fungerar inte som tidigare, alternativt fungerar inte alls. (Kenig m.fl. 2012, 12-14)

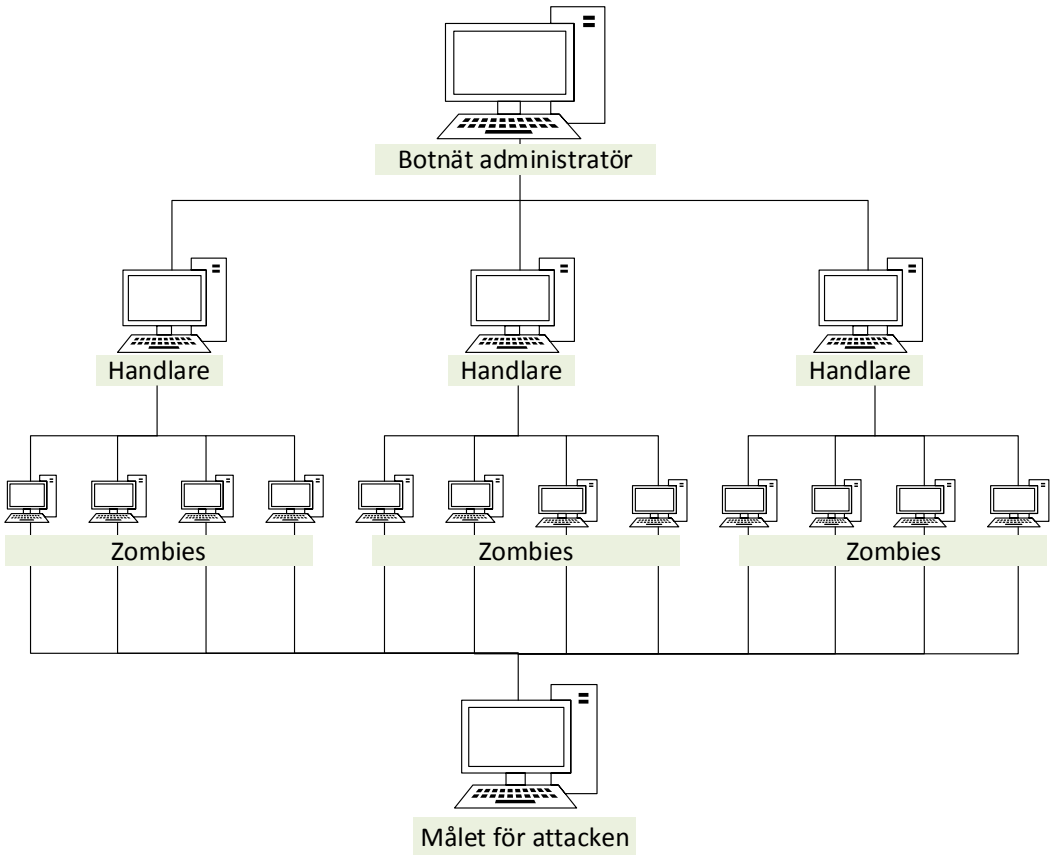
I dagens läge skickas dessa attacker oftast på ett distribuerat sätt. En DDoS-attack använder många datorer och många uppkopplingar, ofta distribuerat i botnät. En DDoS-attack är därför mycket svårare att avleda eftersom det inte bara finns en angripare att försvara sig emot. Det finns i princip två faser i en DDoS-attack. Först utnyttjar hackern internet för att rekrytera datorer att använda i attacken. För att hackern skall kunna lokalisera sårbara datorer hen kan använda sig av under attacken tar hen hjälp av Trojaner och maskar, som letar efter säkerhetshål för att kunna infektera datorerna. Efter att ha rekryterat dessa datorer och då hackern vill lansera attacken skickar han enkla kommandon till de infekterade datorerna för att rikta alla dessa datorers trafik mot ett specifikt mål. (Kenig m.fl. 2012, 7-10)

3.2.1 Botnät

När det kommer till botnät har hackern två olika tillvägagångssätt att välja mellan. Botnät skapas av hackern som använder sig av skadlig kod för att infektera dessa datorer t.ex. genom att skicka e-post med en lockande rubrik som mottagaren genast öppnar och då infekteras datorn. Datoranvändaren märker nödvändigtvis inte av någonting annat än att datorn går långsammare än vanligt. De enskilda datorerna som är en del av ett botnät kallas ofta ”zombies”. Mindre botnät handlar ofta om hundratals infekterade datorer medan större botnät kan innehålla miljontals infekterade datorer. Hackern kan alltså befinna sig var som helst i världen och ändå styra över upp till miljontals datorer.

Det andra nyare alternativet, som också blir vanligare, är att hackern värvar volontärer till att delta frivilligt i attacken.

Även om hackern kan ge enskilda datorer enskilda kommandon, används en mera generell hierarki. En liten del datorer används som ”handlare” vars uppgift var för sig är att kontrollera och kommendera en större grupp datorer. Fördelarna med detta system är att hackern kan skicka ett kommande till en ”handlare” som sedan vidarebefordrar det till datorerna i sin grupp. (Kenig m.fl. 2012, 7-8)



Figur 2. *Illustration över botnätens uppbyggnad.*

3.3 DoS och DdoS

För internetleverantörens kund är bredbandsuppkopplingen deras förbindelse till internetleverantören. Vanligtvis har denna anslutning en lägre kapacitet än anslutningen inom och mellan internetleverantörens routrar. Det här betyder att det är möjligt att internetleverantören kan ta emot en stor mängd trafik och också försöka förmedla den vidare till dess mottagare fast mottagarens anslutning inte klarar av att hantera så mycket trafik. Det i sin tur leder till att mottagarens nätverk överbelastas av trafiken och det leder till att all trafik på mottagarens sida står stilla utan att det behöver drabba internetleverantören nämnvärt. (Stallings & Brown 2008, 250-251)

Den gemensamma nämnaren hos alla typer av överbelastningsattacker är att överbelasta eller krascha nätverket eller tjänsten.

3.3.1 Överbelastningsattacker – tre olika kategorier

Överbelastningsattacker kan delas upp i tre olika kategorier (Stallings & Brown 2008, 250-252);

1. Volymbaserade attacker – Målet med attacken är att överkonsumera bandbredden hos en viss sida och storleken mäts i bitar per sekund. Hit hör till exempel UDP och ICMP översvämningar.
2. Attacker mot ett visst protokoll – Denna typ av attack förbrukar verkliga resurser på en server eller mellanliggande kommunikationsutrustning t.ex. brandväggar och mäts i paket per sekund. Till den här kategorin hör bland annat fragmenterade paket-attacker, SYN översvämningar och Ping of Death-attacker.
3. Attacker mot applikationslagret – Består av förfrågningar, som ser legitima och oskyldiga ut, till en server. Målet är att krascha webbservern genom att skicka så många förfrågningar att den överbelastas. Mäts i förfrågning per sekund. Hit hör HTTP översvämningar.

Typiskt för DoS-attacker mot systemresurser är att syftet alltid är att överbelasta eller krascha mjukvaran som hanterar nätverket. Istället för att konsumera bandbredd med mycket trafik, skickas en speciell typ av paket som konsumerar systemets tillgängliga resurser. En annan typ av attacker mot systemresurser är paket, vars struktur utnyttjar en svaghet i systemet, med syfte att krascha systemet. Det innebär att systemet inte längre kan kommunicera över nätverket förrän mjukvaran är omstartad.

En attack mot en specifik applikation, till exempel en webbserver, innebär normalt ett visst antal förfrågningar, där varje förfrågning konsumerar en stor mängd resurser hos en applikation. Det innebär att webbservern får för många förfrågningar och hinner inte svara på alla.

Enligt en undersökning gjord av Arbors Network växte DDoS-attacker mot applikationer, som utnyttjar egenskaperna hos allmänt använda program-främst HTTP, DNS, HTTPS och SMTP under 2012. Även om dessa attacker förbrukar mindre bandbredd än volymetriska attacker, är de svårare att upptäcka. Arbor ser också en ökning inom multivektor attacker. Under 2011 upplevde 27 procent av de tillfrågade i Arbors årliga undersökning att de hade upplevt multivektor attacker. 2012 svarade 46 procent av de tillfrågade att de har upplevt multivektor attacker. (Anstee, Bussiere, Sockrider, Morales 2013, 24-25)

3.4 Skydd mot överbelastningsattacker

Inom informationssäkerhetsbranschen använder man termerna IDMS, Intelligent DDoS Mitigation System och AMS, Attack Mitigation System, när man pratar om anti-DoS-lösningar. Ett IDMS-/ADM-systems uppgift är att arbeta och undersöka nätverkstrafiken på lager-nivå inom OSI-modellen, samt rapportera till nätverks-administratören hur trafiken ser ut. Eftersom att överbelastningsattackers trafik skickas via olika datakommunikationsprotokoll inom OSI-modellen, är det bäst att bekämpa dessa attacker på lagernivå. IDMS-/ADM-system finns på sidan om nätverket och övervakar nätverkstrafik på många olika punkter samt ger en översyn av säkerhetstillståndet för nätverket. (Arbor Networks Inc.. 2012)

Dagens hackers använder sig av en kombination mellan volymetriska och applikations-attacker för att utföra så kallade multi-vektor attacker som orsakar större skada. Enligt Arbor Networks ” Layered Intelligent DDoS Mitigation Systems”-rapport är det bevisat att den bästa platsen att stoppa volymetriska DDoS-attacker ligger i utkanten av internetleverantörens nätverk, alltså innan den skadliga trafiken hinner in i det fysiska nätverket. Vid det laget då trafiken redan har nått det fysiska nätverket är det vanligtvis för sent för att vidta åtgärder eftersom att attacken redan har överbelastat nätverksinfrastrukturen.

Generellt sett finns det tre olika sätt att stoppa eller mildra en DoS-attack: (Stallings m.fl. 2008, 266-267)

- Förebyggande av attack (före attacken):

Denna lösning gör det möjligt för offret att uthärda attacken utan att behöva förneka service till berättigade kunder. Lösningen inkluderar genomgående regler för resursförbrukning och möjligheten att erbjuda backup-resurser enligt behov. Dessutom modifierar dessa förebyggande åtgärder system och protokoll på internet för att reducerar risken för DDoS-attacker.

- Identifiering och filtrering av attack (under attacken):
  Lösning som försöker upptäcka attacken och svarar mot den direkt. Detta minimerar effekten av attacken. Identifieringen involverar ett ständigt sökande av misstänkt trafik och beteende. Försvarsåtgärder mot attacken sker genom filtrering av paket som sannolikt tillhör attacken.
- Spårning och identifiering av attackens källa (under och efter attacken):
  Detta är ett försök till att identifiera varifrån attacken kommer som ett första steg mot att hindra framtida attacker. Vanligt för denna metod är att den inte genererar resultat tillräckligt snabbt, om den alls ger resultat.

3.4.1 Brandväggar och IPS

DoS är ett kraftfullt sätt att attackera och att förhindra eller mildra DoS-attacker är ingen lätt uppgift. Bästa stället att placera DoS-detektionssystem är på utkanten av internetleverantörens nätverk. Ett av de största problemen med många DoS-attacker är att hackern använder sig av falska IP-adresser. Detta gör det svårt att spåra varifrån attacken kommer. (Stallings m.fl. 2008, 253-254)

Många företag och operatörer tror att de är skyddade mot DDoS-attacker genom att de använder brandväggar och datasäkerhetssystem. Sanningen är att dessa säkerhetsåtgärder faktiskt exponerar företag och operatörer, alltså gör det lättare för hackers att uppmärksamma och upptäcka dem. IPS-system, brandväggar och andra säkerhetsåtgärder *är* viktiga men de är inte utformade för att upptäcka DDoS-attacker. En brandvägg fungerar som en polis som förhindrar obehörig åtkomst till data. IPS-system blockerar icke-auktoriserade försök till att ta sig in på nätverket, som skulle kunna orsaka datastöld. En överbelastningsattack huvudsakliga syfte är inte att stjäla data. Dessutom är IPS-system och

brandväggar statiska lösningar vilket innebär att de oftast är själva målet för DDoS-attacker. (Kenig m.fl. 2012, 43-44)

Ett IPS-system kan jämföras med en brandvägg. Till exempel i ett företags brandvägg finns ett visst antal regler. Dessa regler består av kriterier och om paketet uppfyller dessa kriterier så skickar brandväggen paketet vidare till mottagaren. De främsta funktionerna hos en brandvägg är att förhindra nätverkstrafik från en icke betrodd avsändare. IPS-system kontrollerar också trafiken genom olika regler men dess största uppgift är att leta efter avvikande trafik och vidta åtgärder ifall den upptäcker misstänkt trafik. Problemet med en DDoS-attack är att trafiken kan se legitim ut för en brandvägg eller en IPS-enhet, och på så vis tillåter den skadlig trafik utan att själv veta om det. Säkerhetsprodukter som IPS-system och brandväggar hanterar effektivt nätverkets integritet och sekretess men de misslyckas med att skydda nätverket mot DDoS-attacker. IPS-system och brandväggar är konfigurerade för att tillåta samma protokoll som hackers använder sig av vid DDoS-attacker.

IPS-enheter är särskilt sårbara för översvämnings-attacker eftersom de förlitar sig på resurser som minne och processorkraft för att effektivt fånga paket, analysera trafik och rapportera skadliga attacker. Genom att översvämma ett nätverk med trafik kan en hacker tömma hela IPS-enheten på sina resurser. Under de senaste åren har antalet volymetriska DDoS-attacker ökat markant. Storleken på dessa attacker växer från år till år och de är fortfarande ett stort hot mot företag och operatörer.

Säkerhetsprodukter som IPS-system och brandväggar hanterar effektivt nätverkets integritet och sekretess men de misslyckas med att hantera nätverkstillgänglighet. IPS-system och brandväggar är konfigurerade för att tillåta samma protokoll som hackers använder sig av vid DDoS-attacker.

I början av 2012 släppte Radware ERT sin årliga säkerhetsrapport som baserade sig på de DDoS-attacker teamet varit med om under 2011. ERT-teamet kontrollerade vilka nätverksenheter som varit flaskhalsar under dessa DoS-attacker och fann att i 32 % av fallen var målet organisationens brandvägg och

IPS-enheter. Brandväggar är tillståndsstyrda, vilket innebär att de håller koll på status i de nätverksanslutningar de har som uppgift att kontrollera. Om det inte finns en särskild anti-DoS-enhet, för skydd mot DoS-attacker, kommer brandväggen att öppna en ny anslutning för varje anslutningsförsök som hackern skickar vilket leder till att brandväggens resurser utarmas snabbt. När brandväggens anslutnings-tabell nått sin maximala kapacitet kommer den inte att tillåta att nya anslutningar öppnas och blockerar således också legitim trafik.

4 25 OLIKA TYPERS ÖVERBELASNINGSATTACKER

4.1 25 olika överbelastningsattacker

Som tidigare nämnt kan dessa attacker delas upp i tre olika kategorier beroende på attackens tillvägagångsätt; Volymbaserade, attacker mot ett visst protokoll och attacker mot applikationslagret. Enligt IDMS-tillverkaren RioRey finns det 25 olika sorters överbelastningsattacker. (RioRey Inc. 2011)

Attacktyper		IP-typ	Hand-skakning	Paket-hastighet	Paket storlek
TCP baserade	1. SYN Flood	Falsk	Nej	Hög	Liten
	2. SYN-ACK Flood	Falsk	Nej	Hög	-
	3. ACK & PUSH ACK Flood	Falsk	Nej	Hög	-
	4. Fragmented ACK	Falsk	Nej	Medel	Stor
	5. RST eller FIN Flood	Falsk	Nej	Hög	-
	6. Synonymous IP	Falsk	Nej	Hög	-
	7. Fake Session	Falsk	Nej	Låg	-
	8. Session attack	Icke-förfalskad	Ja	Låg	-
	9. Misused Ap-plication	Icke-förfalskad	Ja	Varierande	-
TCP HTTP baserade	10. HTTP frag-mentation	Icke-förfalskad	Ja	Väldigt låg	Liten
	11. Excessive VERB	Icke-förfalskad	Ja	Hög	-
	12. Excessive VERB Single Ses-sion	Icke-förfalskad	Ja	Låg	-
	13. Multiple VERB Single Re-quest	Icke-förfalskad	Ja	Väldigt låg	Stor
	14. Recursive GET	Icke-förfalskad	Ja	Låg	-

	15. Random Recursive GET	Icke-förfalskad	Ja	Låg	-
	16. Faulty application	Icke-förfalskad	Ja	Låg	-
UDP baserade	17. UDP Flood	Falsk	-	Väldigt hög	Liten
	18. Fragmentation	Falsk	-	Väldigt hög	Stor
	19. DNS Flood	Falsk	-	Väldigt hög	Liten
	20. VoIP Flood	Falsk	-	Väldigt hög	Liten
	21. Media Data Flood	Falsk	-	Väldigt hög	Medel
	22. Non-Spoofed UDP Flood	Icke-förfalskad	-	Väldigt hög	-
ICMP Baserade	23. ICMP Flood		-	Väldigt hög	Varierande
	24. Fragmentation		-	Väldigt hög	Stor
	25. Ping Flood		-	Väldigt hög	Liten

Tabell 1. De 25 olika attacktyperna.

4.1.1 Översvämningar

Översvämningsattacker utförs i olika former, baserat på vilket nätverksprotokoll som används för att genomföra attacken. Det gemensamma målet för alla översvämningsattacker är att överbelasta nätverkskapaciteten hos en server. Dessa attacker översvämmar nätverksanslutningen till servern med ett flöde av värdelösa paket. Virtuellt sett kan alla typer av nätverkspaket användas vid översvämningsattacker. De behöver bara sådana paket som har tillåtelse att trafikera till servern. Ju större paket desto effektivare bli attacken. De vanligaste översvämningsattackerna använder sig av ICMP-, UDP- eller TCP SYN-pakettyper. (Stallings m.fl. 2008, 257-260)

I dataålderns början tilläts ICMP-paket av nätverksadministratörer eftersom att ping-kommandot är ett enkelt och användbart nätverksdiagnostiseringsverktyg. På senare tid har nätverksadministratörer börjat begränsa antalet tillåtna ICMP-paket som får passera genom brandväggen. En hacker kan generera stora mängder av denna pakettyp. Eftersom dessa paket inkluderar en del felaktiga paket ökar deras effektivitet i översvämningen på grund av att felaktiga paket kräver mera system-resurser. (Kenig m.fl. 2012, 27-28)

En annan sorts attack är ICMP-paket och UDP-paket som skickas till ett visst portnummer hos måltavlan. En vanlig UDP-attack utförs genom att hackern skickar ett UDP-paket till ping-tjänsten hos en server. Om servern kör den tjäns-ten så svarar den med ett UDP-paket tillbaks till avsändaren. Om tjänsten inte körs så förkastas paketet. Men genom att hackern skickar flera paket än servern hinner svara på blir UDP-porten snabbt täppt av trafiken. (Kenig m.fl. 2012, 27-28)

En DNS översvämning är lätt att starta och svår att upptäcka. Baserat på samma idé som andra översvämningsattacker, riktar en DNS flood trafiken mot DNS programprotokoll genom att skicka en stor mängd DNS-förfrågningar. DNS är protokollet som används för att översätta domännamnet till en IP-adress och vice versa. Under en DNS översvämning skickar angriparen upprepade DNS-förfrågningar, antingen direkt eller via ett botnät, till offrets DNS-server som blir oförmögen att bearbeta eller besvara de förfrågningar som den får och så småningom kraschar den. (Stallings m.fl. 2008, 264-265)

Genom att skicka många TCP-anslutningsförfrågningar, antingen med riktiga eller falska avsändaradresser, till systemet får hackern systemet överbelastat. Hackers utför också TCP-attacker genom att skicka TCP-datapaket mot systemet vilket leder till överbelastning. Fast systemet kan förkasta dessa paket så hinner systemet inte med.

4.1.2 Svagheter inom TCP/IP-protokollet

Dessa attacker missbrukar TCP/IP-protokollet genom att dra nytta av brister i dess utformning. De missbrukar oftast de 6 kontrollbitarna i TCP/IP-protokollet; - SYN, ACK, RST, PSH, FIN och URG med syfte att förstöra de normala mekanismerna för TCP-trafik. Till skillnad från till exempel UDP- och andra anslutningslösa protokoll, är TCP/IP anslutningsbaserad som betyder att paketavsändaren måste etablera en anslutning med mottagaren före hen kan skicka paket. TCP förlitar sig på en tre-vägs-handskakning mekanism(SYN, SYN-ACK, ACK) där varje förfrågning skapar en halvöppen anslutning(SYN), en förfrågan om ett svar (SYN-ACK), och sedan meddelande om svaret (ACK). Vid attacker mot TCP skickar hackern paket till TCP men i fel ordning, vilket leder till att servern tömmer sina resurser och trafiken står stilla. (Kenig m.fl. 2012, 29-31)

4.1.3 HTTP, HTTPS och SSL/TLS

Många företag använder sig av SSL/TLS-protokollet för att kryptera trafik som rör sig mellan olika applikationer inom egna nätverket. Antalet DDoS-attacker mot krypterad trafik stiger och att mildra dem är inte så lätt som man kunde förvänta sig. De flesta DDoS-riskreducerande tekniker som används inspekterar inte alls SSL trafiken, eftersom det kräver att man först dekrypterar den krypterade trafiken. HTTPS-floods, som alltså är krypterad HTTP-trafik, syns oftare i Radwares attackstatistik /3, 33-34/. Förutom de ”normala” HTTP översvämningarna så utmanar HTTPS översvämningar på andra sätt bl.a. genom utmatta krypteringen och dekrypteringen.

I och med den ökade användningen av SSL, en metod för kryptering som används av olika nätkommunikationsprotokoll, har hackers börjat rikta direkta attacker också mot krypterade SSL-asnlutningar. SSL körs över TCP/IP, och ger säkerhet till användare som kommunicerar över andra protokoll genom att kryptera sin kommunikation och autentisera de kommunicerande parterna. SSL-baserade DoS-attacker tar sig många former; inriktning mot SSLhandskakningen, skickar meningslös data till en SSL-server, eller missbrukar vissa funktioner relaterade till den krypterade SSL-förhandlingsprocessen. SSL-baserade attacker kan också helt

enkelt betyda att en DoS-attack lanseras över SSL-krypterad trafik vilket gör dem extremt svårt att identifiera. Sådana attacker betraktas som "asymmetriska", eftersom det krävs betydligt mer resurser på servern för att hantera en SSL-baserad attack än det gör för att lansera en. (Kenig m.fl. 2012, 33-35)

4.1.4 Low and slow-attacker

Low and Slow-attacker kräver ingen stor mängd trafik. De riktar attacken mot specifika konstruktionsfel eller sårbarheter på en server med en relativt liten mängd av skadlig trafik, som småningom orsakar att servern kraschar. Low and Slow-attacker riktas främst till programresurser, ibland också serverresurser, och är mycket svåra att upptäcka eftersom de använder anslutningar och dataöverföring som tycks ske i normal takt. (Kenig m.fl. 2012, 35)

4.1.5 TDoS och VoIP Flood

Hackers har länge kunnat nässla sig in i datornätverk från olika håll. Även om företag ofta är noggranna med att skydda sitt nätverk finns det ett område som ofta förbises, nämligen VoIP-system. Liksom Dos-attacker är TDoS-attacker försök att täppa till linjer och avbryta regelbunden verksamhet med en stor mängd trafik.

Jämfört med stora DDoS-attacker kräver TDoS-attacker varken stora datorresurser eller teknisk kunskap, verktygen finns på internet. Det är lätt att täppa till en telefonlinje genom att helt enkelt ringa samma nummer om och om igen. Hackers använder oftast VoIP-automatiseringsskript för att utföra dessa attacker. (Nachreiner 2013)

4.2 Vem ligger bakom dessa attacker och vad är motiven?

Verktyg och instruktioner för att utföra överbelastningsattacker är lätta att hitta och ladda ner från Internet. Vem som helst kan ladda ner dem och vem som helst kan använda dem, och det gör människor också. Tillgängligheten och medvetenhet om dessa verktyg och instruktioner har gjort DDoS-attacker tillgängliga för vem som helst. (Kenig m.fl. 2012, 16)

4.2.1 Ekonomisk vinning

Enligt en undersökning gjord av Arbor är de tre största motiven bakom attackerna politiskt motiverade, riktade mot online-spelande och vandalism. Organisationer som använder DDoS-attacker för att uppnå ekonomisk vinning kan delas in i två kategorier; de som har för avsikt att få en fördel gentemot sina konkurrenter och de som försöker utföra brottslig utpressning. Det finns organisationer som säljer DDoS-attack-tjänster till privatpersoner såväl som till företag. (Anstee m.fl. 2013, 89-90)

Kriminell utpressning genom DDoS-attacker börjar med att DDoS-attack-köparen väljer ett mål för DDoS-attacken. Sen avfyras en liten DDoS-attack mot deras nätverk. Det attackerarande företaget kommer då att skicka ett meddelande till målet, att de har möjlighet att betala ”lösensumma” för att undgå mera allvarliga attacker. Om det attackerade företaget går med på att betala, riskerar de bli stämplad som "betalare" genom DDoS-for-hire service och blir en lätt måltavla för framtida utpressningsförsök. I denna situation blir det ofta nödvändigt att använda någon form av anti-DDoS-lösning för att förhindra framtida attacker.

4.2.2 Politiska motiv

Bortsett från ekonomisk vinning, genom att slå ut sina konkurrenter samt stulna kreditkort, har det under senare år också skett en ökning av politiskt motiverade DDoS-attacker runt om i världen, främst Iran, Sydkorea, Estland, Malaysia, Kina och USA. Dessa relativt nya motiv markerar en utveckling inom cyberattacker som kallas ”hackitivism”. The Anonymous är en relativt känd hackitivism-grupp som oftast attackerar anhängare av lagstiftning de anser ogynnsamma och olika statliga organ med anknytning till sådan lagstiftning. ”Operation Payback” var en serie cyberattacker initierade av Anonymous, som hämnd för den amerikanska regeringens tillslag mot Wikileaks som hade exponerat konfidentiellt material om regeringens dokument och kommunikation. Under ”Operation Payback” riktade Anonymous DDoS-attacker mot webbplatser som bl.a. Visa, MasterCard, PayPal, CBS och FBI. Det huvudsakliga syftet med dessa attacker var att protestera mot orättvisor. Det unika med ”Operation Payback” var att Anonymous för första

gången, på stor skala, rekryterade frivilliga att ladda ner ett speciellt DDoS-verktyg som tillät dem att delta i attacker med en mera erfaren hacker. (Kenig m.fl. 2012, 17-19)

Det verktyg som Anonymous oftast använder vid sina attacker är Low Orbit Ion Cannon, LOIC, ett enkelt översvämnings-verktyg, som generera massiva mängder av TCP, UDP eller HTTP-trafik i syfte att utsätta en server till för stor belastningen på nätet. Medan LOICs ursprungliga utvecklare, Praetox Technologies, avsett att verktyget kan användas av utvecklare som bara vill testa att utsätta sina egna servrar för en sådan tung nätverkstrafik, plockade Anonymous upp opensource-verktyget och började använda den för att lansera samordnade DDoS attacker. (Kenig m.fl. 2012, 38-39)

4.3 Vad är resultatet av dessa attacker?

Antalet DDoS-attacker stiger och attacker som orsakar avbrott över 12 timmar för den utsatta organisationen är inte ovanligt. Därför bör man ta hänsyn till risker och de ekonomiska konsekvenserna av en avbrottstid för 24 timmar.

Saker man bör ta i beaktande enligt Arbor är (Arbors Networks Inc. 2013):

Driftskostnader: Hur många anställda kommer inte att kunna sköta sitt arbete om nätverket är nere och hur mycket kostar det för företaget per timme?

Helpdesk: Om systemen ligger nere, hur många flera samtal skulle komma till Helpdesken och hur mycket pengar skulle dessa samtal inbringa till företaget? Hur mycket pengar skulle företaget gå miste om per timme ifall Helpdesk-telefonlinjen ligger nere?

Återhämtning: Hur mycket arbete krävs det för att reparera systemen och vad kostar det för företaget?

Förlorade affärer: Hur mycket affärer kommer företaget att gå miste om per timme?

Förlorade kunder: Hur många existerande kunder kommer att byta operatör/ köpa tjänster av ett annat företag? Vad är livstidsvärdet på dessa kunder?

Förlorade framtida affärer: Hur mycket kommer förmågan att locka nya kunder skadas? Vad är värdet på dessa förlorade affärer?

Skador på företagets image och rykte: Hur mycket kostar det företaget?

Efter att ha utvärderat dessa nyckelfrågor har företaget fått en uppfattning om hur verksamheten finansiellt skulle påverkas av en DDoS-attack. Och eftersom målet med en DDoS-attack är att skapa så mycket skada som möjligt är det högst troligt att en attack inträffar på värsta tänkbara tidpunkt för företaget t.ex. inom teknologisektorn kunde en attack ske samma dag som en stor ny produkt lanseras. Internetleverantörer kan få en unik fördel genom att erbjuda övervakningsbara lösningar, för att bekämpa både volymetriska attacker och attacker på applikationslagret, till sina kunder. (Arbors Networks Inc. 2013)

5 EN JÄMFÖRELSE MELLAN TRE OLIKA IDMS-SYSTEM

I den här delen av lärdomsprovet får läsaren ta del av information om tre olika IDMS-lösningar från tre olika företag specialiserade på skydd mot DDoS-attacker. Här beskrivs hur de fungerar, fördelar och nackdelar och om det är kompatibelt med Anvia ICTs nätverk.

5.1 Arbor Networks

Arbor Networks Inc. beskriver sig själva som en global ledare inom nätverkssäkerhet. Arbor Networks grundades efter banbrytande forskning som bedrevs vid University of Michigan, USA, på uppdrag av US Defense Agency Reasearch Projects Administration, USA, under 1990-talet. Sedan dess har Arbor Networks Inc. fortsatt att fokusera på forskning. Arbor Network Inc.s lösningar finns globalt tillämpade hos stora operatörer och internetleverantörer men även hos webbhotell och leverantörer av molntjänster hittar man Arbor Networks lösningar.

Det som skiljer Arbor från andra nätverkssäkerhetsföretag är deras ATLAS-system. ATLAS är ett samarbetsprojekt mellan Arbor och flera än 230 operatörer och internetleverantörer som har kommit överens om att sinsemellan dela känsliga nätverkstrafikdata med Arbors Security Engineering & Response Team, ASERT. Arbor är idealiskt positionerade för att ständigt vara uppdaterade och kunna leverera information om DDoS och botnät till sina kunder. Sedan starten har Arbor jobbat med världens mest krävande operatörer och hjälpt dem att förstå, identifiera och mildra nätbaserade hot mot deras verksamhet.

5.1.1 Arbor Networks Peakflow SP

Arbor Networks Peakflow SP är en säkerhetsplattform som gör det möjligt för internetleverantörer och stora företag att möta dagens behov på säkerhetslösningar mot DDoS-attacker. Som det första systemet som i stor utsträckning integrerar hela nätverket i deras system, både identifierar och stoppar både volymetriska attacker och attacker mot applikationslagret utan att avbryta den legitima trafiken.

Arbor Network Peakflow SP är Arbors IDMS-lösning som riktar sig främst till operatörer och internetleverantörerer. Peakflow SP är baserad på följande principer:

- Känn ditt nätverk: Att ha en genomträngande syn över nätverket, applikations- och routintrafik gör det möjligt att fatta välgrundade beslut om nätverksarkitektur, kunder och nya IP-tjänster.
- Säkra din infrastruktur: Realtidsdetektion och begränsning av säkerhetshändelser gör det möjligt att förhindra negativ inverkan på nätverket, data, tjänster och kunder.
- Utveckla och öka din verksamhet: Utnyttja samma Peakflow SP platform, som används för nätverkssynlighet och säkerhet, för att leverera enskilda rapporter över nätverkets tillstånd.

Peakflow SP meddelar operatörer om följande saker:

- Var trafiken på deras nätverk kommer ifrån och vart den är på väg.
- Vilken väg trafiken går.
- Vilka gränssnitt och anordningar som används mest.
- Vem använder mest trafik i nätverket.
- Vad är/har varit trenderna under kort och lång tid.
- Rapporterar prognoser över hur nätverkstrafiken ser ut.

En av Peakflows största fördel är dess förmåga att generera varningar över alla abnormiteter i nätverket. Dessa avvikelser kan vara ett tecken på en DDoS-attack, enheter som inte fungerar normalt eller felkonfigurationer. Dessa varningar gör att operatören kan upptäcka problemen snabbt, snabbt identifiera orsaken och vidta åtgärder.

5.1.2 Arbor Networks Peakflow SP teknisk information

Komplett består Peakflow SP lösningen av fem olika anordningar:

1. Peakflow SP collector Platform (CP): CP 5500-5, CP 5500-2:
- Ger central administration, rapportering och alarm inom Peakflow SP.

- Kan användas endast som en dataflöde-uppsamlare eller som både dataflöde-samlare och som administrations platform i en utplacerad Peakflow SP.

2. Peakflow SP Flow Sensor (FS): FS 5500:

- Utför insamlingen och analysen av datan

3. Peakflow SP Portal Interface (PI): PI 5500:

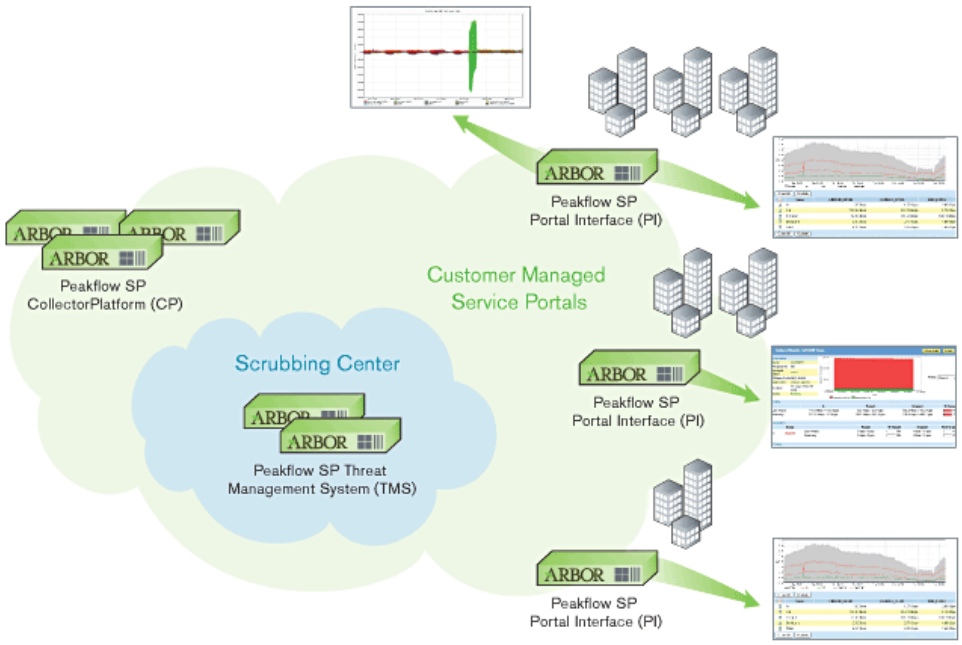
- Administrations platform för händelser inom Peakflow SP
- Avlastar hantering och rapportering från CP-apparaten (punkt 1.)
- Designad för att stödja även kundernas portaler alternativt egna övervakningsverktyg samt stödjer användningen av flera användare samtidigt.

4. Peakflow SP Business Intelligence (BI): PI 5500

- Administrationsplatform för att skapa övervakade och skyddade objekt, dvs. kunder, nätverk, resurser.

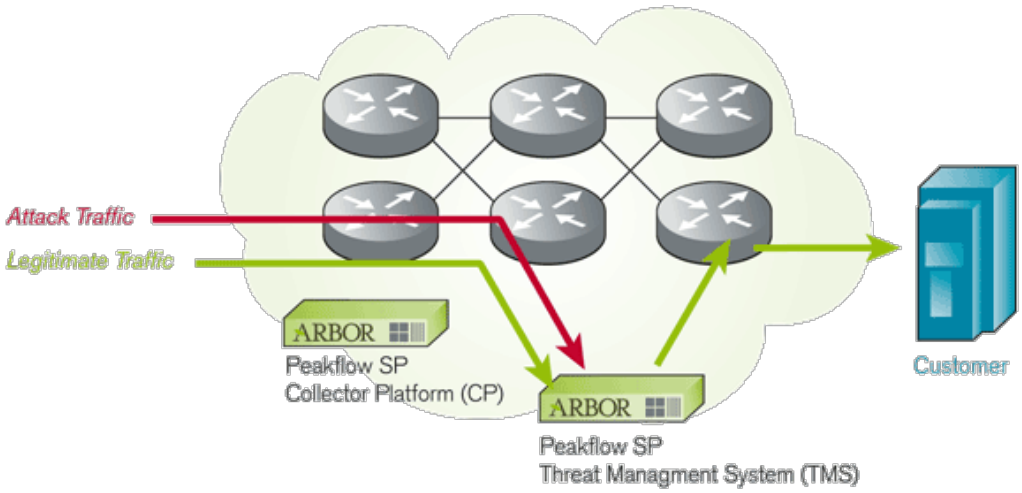
5. Peakflow SP Threat Management System

- En samling DDoS-riskreducerande apparater alternativt inbäddade i routrar (Alcatel Lucent 7750 SR eller Cisco CRS)
- Bidrar till DPI, Deep Packet Inspektion, applikations-intelligens samt kirurgisk lindring av attacker.



Figur 3. Illustration över samtliga Arbor Networks Peakflow SP-maskiner i drift.

5.1.3 Hur fungerar det?



Figur 4. Illustration över hur Arbor Networks Peakflow SP hanterar den skadliga trafiken.

Peakflow SP CP, som är lokaliserad I utkanten av nätverket, är den första som uppmärksammar avvikande trafik. Vanligtvis låter Peakflow SP CP trafiken gå

vidare in till nätverket men om den upptäcker avvikande trafik så skickar den vidare trafiken till Peakflow SP TMS. Peakflow SP TMS fungerar som en tvättmaskin. På engelska kallas den för ”scrubbing machine”. En maskin som skrubbar bort den dåliga trafiken och låter legitim trafik passera vidare till nätverket.

5.2 RioRey

RioRey Inc. är ett privatägt företag med huvudkontor i Maryland, USA. RioRey designar, utformar och tillverkar en heltäckande produktlinje av dedikerade enheter vars uppgift är att försvara nätverk från DDoS-attacker. RioRey har en egen teknologi kallad ”algorithmic centric” som är känd som nästa generations lösning på DDoS-attacker. RioReys produkter är anpassade för att fungera med små och medelstora företag, myndigheter, operatörer och webbhotell världen över.

Innan RioRey började utforma sitt system utvecklade de en konceptuell modell av en DDoS-attack och dess beteende. RioRey visste att attackerna skulle öka i antal, storlek och komplexitet. Därför skulle inte vanliga säkerhetsplattformar som behandlar många olika säkerhets- och nätverks relaterade problem, t.ex. brandväggar, inte vara hållbara för att skydda mot DDoS-attacker. Summan av kardemumman blev att RioRey byggde en speciell säkerhetsplattform vars enda uppgift är att skydda kunden från DDoS-attacker.

5.2.1 RioRey RS 30

RioRey RS-serien innehåller kraftfulla verktyg mot DoS-attacker. RS-serien kan skydda nätverk som omfattar upp till 100 Gbps på 32 miljoner paket per sekund. rView är RioReys egna mjukvara som fungerar som ett rapporteringsverktyg för alla RioRey komponenter som finns installerade på nätverket. rView bidrar till fullständigt nätverkssynlighet genom fullständig information om DDoS-attacker samt sammandragsrapporter över både realtid och bakåt i tiden. RioRey RS30 är noggrant uppvecklad under flera år.

5.2.2 Hur funkar det?

Som kund installerar man först RioRey RS30-switch på utkanten av sitt nätverk. Där övervakar RS30 alla trafik som är på väg in till nätverket. RS 30 är uppbyggd på en mjukvara som består av 33-34 olika noggrant utvecklade algoritmer. Genom dessa algoritmer kontrollerar RS30 trafiken. Om algoritmen säger att trafiken är skadlig kommer RS30 att dumpa trafiken om algoritmen anser trafiken vara legitim skickas den vidare in på nätverket.

RS30 har alltså inget scrubbing-center som är vanligt hos övriga IDMS-tillverkare.

5.3 RADWare

Radware är en global ledare inom leverans och tillämpade säkerhetslösningar för virtuella och molnbaserade datacenter. Dess prisbelönta lösningar ger full motståndskraft mot affärskritiska applikationer, maximal IT-effektivitet och fullständig affärsrörlighet. Radwares organisations-anpassade lösningar finns i dagens läge i över 10 000 företag världen över. För Radware ät det viktigt att anpassa sig till marknadens nya utminaningar snabbt, upprätthålla kontinuitet i verksamheten och uppnå maximal produktivitet samtidigt som kostnaderna hålls nere.

RADWare har ett scrubbingcenter i Tyskland, dit oönskad och illegitim trafik dirigeras. RADWare har också ett Emergency Response Team (ERT) lokaliserat i Israel. ERT-teamet finns tillgängligt dygnet runt, året om, och om man upplever en större DDoS-attack kan man kontakta dem för hjälp.

5.3.1 RADWare DefensePro x420

Med möjligheten att hantera upp till 25 miljoner paket per sekund under en DoS-attack, oavsett paketets storlek, samt upp till 40Gbps av legitim trafik, erbjuder Radwares lösning DefensePro X420 världens effektivaste anti-DoS-lösning. DefensePron X420 är utformad för att skydda organisationer från de kraftigare överbelastningsattackerna. Tack vare sin höga kapacitet kan DefensePro X420 tillgo-

dose behoven till och med hos de största online-företagen, tjänsteleverantörer och operatörer.

DefensPro X420 innehåller en uppsättning säkerhetsmoduler så som IPS, NBA, DoS-skydd och ryktesmaskin, för att kunna skydda nätverket och hantera hot mot nätverket till 100 %. Kärnan i DefensePro X420 är en beteende-baserad realtids-teknologi som upptäcker och tar hand om attacker på under 18 sekunder. Allt utan mänsklig inblandning och utan att blockera legitim trafik. Defensepro använder en dedikerad hårdvaruplattform baserad på Radware OnDemand-switch som stöder nätverkesgenomströmningar upp till 40Gbps. Det bäddar in två olika dedikerad hårdvarukomponenter: en DoS Mitigation Motor (DME) för att förhindra hög volym av DoS- och DDoS-översvämning attacker, utan att påverka legitim trafik. StringMatch Motor (SME) uppgift är att snabbare upptäcka suspekta signaturer på datapaket.

Apsolute Vision är RADWare rapporterings- och övervakningslösning till DefensePron. Den erbjuder ett centraliserat för administration, övervakning och rapportering inom de DefensePron man har installerade i nätverket. Den bistår användaren med realtidsidentifiering, prioritering och svar på regelbrott, cyberattacker och insiderhot.

5.3.2 Hur fungerar det?

DefensePro X420 fungerar i det stora hela som övriga anti-DoS-lösningar dvs. DefensPro-switchen placeras i utkanten av nätverket och dess uppgift är att följa trafiken och om den upptäcker onormal trafik styr den trafiken till scrubbing-centret. När man tar DefensePro x420 i bruk rekommenderas att switchen kopplas in i nätverket åtminstone en vecka på förhand innan man tar i bruk anti-DoS-egenskapen. Detta görs för att under den ena veckan följer DefensePron med trafiken och registrerar hur nätverket ser ut, vilka tider förekommer det mest trafik, hurudan trafik förekommer osv. När sedan anti-DoS-egenskapen kopplas på jämför DefensePron all trafik med sitt register från första veckan. Om trafiken inte är jämförbar med registret skickas trafiken vidare till scrubbing-centret.

Detta skulle kunna ses som ett problem eftersom det vid diverse större tillställningar, t.ex. en webbsänd ishockey VM-match, som automatiskt drar till sig en stor mängd trafik och som inte DefensePron hunnit bekanta sig med. Enligt Robert Seimann, Technical Account Manager på Radware Ltd., är detta inget problem för DefensePron eftersom den inte bara förlitar sig på datamängden utan även på hur trafiken ser ut och varifrån den kommer.

6 SLUTSATSER OCH RESULTAT

En anskaffning av en IDMS-lösning handlar om en 6-siffrig investering. Anvias styrelse vill förstås gärna se en sådan stor investering betala tillbaka sig. I dagens läge är det svårt att se vad dessa attacker kostar Anvia och således utreda vilken nytta en anti-DoS-lösning ekonomiskt sett skulle ha för Anvia. Man kan jämföra en IDMS-lösning med en hemförsäkring. Det känns inte alltid lönsamt att betala hundratals euro per år i försäkringar då ens hus ändå aldrig brinner ner. Men om huset skulle brinna ner så är du glad över att du betalt försäkringspremierna.

Även fast en anti-DoS-lösning är en stor investering skulle Anvia kunna sälja anti-DoS-lösningen vidare till sina kunder. Till exempel genom att i nätverket välja att tillåta attacker under 500 Mbps och låta anti-DoS-lösningen hantera endast attacker över 500 Mbps. Då skulle kunden kunna investera i ett tilläggsskydd från Anvia, till exempel om kunden inte alls vill tillåta attacker i sitt nätverk kan han köpa en IDMS-lösning av Anvia. På så sätt skulle en IDMS-införskaffning även inbringa direkt inkomst till Anvia. Detta är möjligt med samtliga tre tillverkar som jämförelsen gjort mellan.

6.1 Resultat av jämförelsen

Jämförelsen visar att alla dessa tre olika IDMS-system ger ett fullgott skydd mot DDoS-attacker. De tre systemen är uppbyggda på olika sätt och den största skillnaden är hur de tar hand om trafiken. Arbors och RadWares lösning liknar varandra i och med att de båda tar hand om den skadliga trafiken genom att skicka den till ett scrubbing-center medan RioReys lösning tar hand om trafiken på helt annat sätt. Det som också skiljer dem åt är tillvägagångssättet för att upptäcka den skadliga trafiken. Arbor har switchar utplacerade runtom i nätverket som kollar trafiken. RadWare ”lär” sina switchar hur normal trafik ser ut för att sedan jämföra all trafik med inlärningsmönstret. RioRey kontrollerar all trafik med hjälp av olika algoritmer för att ta reda på om trafiken är legitim eller inte.

I och med att tillvägagångssättet för att ta hand om den skadliga trafiken skiljer sig mellan dessa system varierar också latenstiden för *när* systemet hittar den

skadliga trafiken och för *när* systemet vidtar åtgärder mot den skadliga trafiken. Till dessa tre olika lösningar finns övervakningssystem och administrationssystem som alla tre innehåller samma funktioner.

Prestanda			
	RADWare DefensePro X420	**Arbor Networks Peakflow SP**	**RioRey RS30**
Max antal paket/sekund	25 000 000 st	inga begränsningar	8 000 000 st
Latens	< 60 mikrosekunder	Trafiken går direkt vidare	< 100 mikrosekunder
Realtid	Upptäcker och skyddar mot angrepp på mindre än 18 sekunder	-	Upptäcker DDoS-attacker inom 30-90 sekunder, vidtar åtgärder inom 90-120 sekunder
Inspektionsportar			
10 GE	20 (SFP+)	8 (SFP+) Dual hard drive RAID 1	6 (SFP+) portar
40 GE	4 (QSFP+)	-	-
Portar för konfigurering			
10/100/1000 Koppar ethernet	2 x RJ45	-	2 x RJ45
Driftläge			
Nätverksdrift	Genomskinlig L2 Forwarding	Diversion/Reinjection (out-of-band) In-Line, Mirror Port	-
Utplacering	In-line, SPAN Portövervakning, kopieringsportsövervakning, lokala utgången, utgångsbegränsning (vid skrubbning-center lösning)	In-line aktiv, Inline övervakning, SPAN port, vidarekoppling/ återföring	In-line eller out-line beronde för kundens nätverksstruktur
Inspektions av tunnlar	VLAN-märkning, L2TP, MPLS, GRE, GTP, IPinIP	-	Inspekterar IP-lasten inne i GRE tunnlar, tunnel rubriker ignoreras

Stöd för IPv6	Ja	Ja	Ja, kräver uppgradering av systemvaran
Blockeringsåtgärder	Droppa paket, reset (källa, destination, båda), upphäva (källa, src-port, destination, destinations port eller någon kombination) Challenge-Response för misstänkt TCP, HTTP och DNS trafik.	Blockering/tillfällig avbrytan mot källan, blockering per paket, kombination av båda. Hastighets-baserad-blockering	Black- och whitelistor av destinations-IP samt källor. 33-34 algortimer som kontrollerar all trafik.
Fysiskt			
Mått (cm)	58,2 x 48,2 x 8,8 cm	8,76 x 45,54 x 51 cm	12 x 48,26 x 57,5 cm
Vikt (kg)	15,1	17,7	154
Strömkällor	AC: 100-120V/200-240V, 47-63 Hz DC: -36 – -72V	AC: 100-127V/200-240V, 50 to 60Hz, 6/3A DC: -48 to -60V, 10A max	110/220V AC eller-48V DC
Drifttemperatur	5-55°C	5°-40°C	10°-50°C
Fuktighet	5 % - 95 % (icke-kondenserande)	5 % till 85%	-
Garanti	1 års hårdvara och mjukvara underhåll	1 års hårdvara och mjukvara underhåll	1 års hårdvara och mjukvara underhåll
Support	Support av ERT-teamet 24/7/365	Support 24/7/365	-

Tabell 2. Jämförelsediagram över PEakflow SP, DefensePro 420 och RS30.

6.1.1 Scrubbingcenter – för- och nackdelar

Duncan Hume säger i under en företagspresentation att det största problemet med skrubbning-center är att skrubbning-center är beroende av bandbredd för att klara av en attack. Om vägen till ett skrubbning-center är en anslutning som rymmer 200Gbps vad händer då en stor kund är under attack på 195 Gbps? Vad händer med resten av kunderna som använder tjänsten? Skrubbning-centret blir då överbelastat av sin egen trafik. Ifall att attacker riktats mot flera av IDMS-tillverkarens kunder är det inte säkert att skrubbning-centret har kapaciteten att

”tvätta” all denna trafik, om anslutningen till scrubbing-centret redan är full. (Hume D. 2013)

Om trafiken skickas till ett skrubbning-center för att ”tvättas” kan det orsaka latens i nätverket. Om skrubbning-centret lokaliserats utrikes medför det enligt Hume också en stor risk för dataintegritets- och säkerhetsbrott. Banker, sjukvård och privata uppgifter av alla slag kan äventyras. Problemet med RioReys lösning är att då den skadliga trafiken blockas kan det lätt uppstå trängsel, beroende på attackens storlek, vid ingången till nätverket. (Hume D. 2013)

7 AVSLUTNING

Tänk dig att du vaknar en morgon, slår på radion och får höra att en utländskhackergrupp har attackerat Finlands transportsystem och elnät. Många städers elsystem har redan inaktiverats, alla serviceföretag och myndigheter tvingas stänga igen.

Detta är ett exempel på hur sårbart IT-samhället är och ett försök till att illustrera cyber-domedagen. Med den ökade integrationen av datorer och datornätverk i samhället är sannolikheten för att en sådan attack inträffar, inte lika astronomiskt liten som för 30 år sedan.

Hela Finlands infrastruktur bygger på datateknik (Järvinen 2012, 14). El- och vattenbolag, banker, butiker, sjukhus, TV- och radiostationer, telefoni och andra vardagliga tjänster är beroende av datateknik för att kunna fungera. I jämförelse med många u-länder är vi i Finland helt beroende av el och dataförbindelser. En effektiv attack skulle kunna få Finland ner på sina knän inom timmar utan att behöva avfyra ett ända skjutvapen.

En mindre dramatisk men lika viktig sak är kriskommunikation. Om något skulle hända så bör myndigheterna kunna informera och ge medborgarna instruktioner snabbt. Det är lättare sagt än gjort om all teknik ligger nere. Den officiella kriskommunikationskanalen i Finland är Radio Yle 1 (Järvinen 2012, 17) men hur många har möjlighet att lyssna på radio mitt i arbetsdagen? Och när människor hör att något har hänt vänder de sig till webben med risk för att nyhetssidorna kollapsar.

Under de närmaste åren räknar Radware med att DDoS-attacker kommer att öka i frekvens, vara mera sofistikerade samt ihärdigare. Kraftfulla DoS- och DDoS-attacker kommer att dra mer nytta av den krypterade SSL-trafiken och rikta dessa attacker mot företag som är beroende av krypterade anslutningar såsom finansiella institutioner, statliga byråer och social media. Varje organisation, vars nätverk och kommunikation bygger på SSL-baserad trafik utan en ordentlig

dekrypteringsmotor som arbetar synkroniserad med en IDMS-lösning, kommer att vara utsatta. (Anstee m.fl. 2013, 51-52)

7.1 Sammanfattning

Lärdomsprovet gjordes på uppdrag av Anvia Abp och dess två huvudsakliga syften har varit att kartlägga DDoS-attacker samt göra en kartläggning över tre olika IDMS-system. Termerna DDoS, DoS och överbelastningsattack har jag känt till sedan tidigare men inte dess mera insatt i deras tillvägagångsätt eller syfte. Under arbetets gång har jag lärt mig mycket om överbelastningsattacker och hur mycket de kan ställa till med. Det har också varit lärorikt och informativt att få närvara vid företagens produktpresentationer.

Avslutningsvis kan jag personligen dra den slutsatsen att överbelastningsattacker är ett ständigt växande hot mot alla, inte bara mot internetleverantören. Dessa attacker blir också kostsamma i längden för företag och därför bör man se över sin datasäkerhetsstrategi.

KÄLLOR

Böcker

Stallings W. & Brown L.. 2008. Computer security Principles and practice. Första upplagan. Upper Saddle River. Pearson education, Inc.

Järvinen P.. 2012. Arjen tietoturva. Första upplagan. Jyväskylä. Docendo.

Elektroniska publikationer

Symantec Corporation. 2013. Internet Security Report 2013. Hänvisat 30.10.2013. Symantec Corporation. USA. Finns att fås via internet. **http://www.iseprograms.com/lib/Symantec-internet-security-threat-report.pdf**

CERT-FI. 2013. Informationssäkerhetsöversikt 1/2013. Hänvisat 13.11.2013. http://www.cert.fi/sv/rapporter/rapporter_13/1_2013.html

Kenig R., Manor D., Gadot Z., Trauner D.. 2012. DDoS Survival Handbook. Hänvisat 30.10.2013. Radware Ltd.. USA. Finns att fås via internet. **http://security.radware.com/uploadedFiles/Resources_and_Content/DDoS_Handbook/DDoS_Handbook.pdf**

Anvia Abp. 2013. Anvia i korthet. Finns att fås via internet. http://www.anvia.fi/sv/om-anvia/info-om-anvia/grundinformation-om-anvia/anvia-i-korthet

Anvia Abp. 2013. Anvia ICT. Finns att fås via internet. http://www.anvia.fi/sv/anvia/info-om-anvia/affarsomraden/anvia-ict

Arbor Networks Inc.. 2012. Layered Intelligent DDoS Mitigation Systems. Finns att laddas ner. http://www.arbornetworks.com/resources/media-library/provider-materials

Anstee D., Bussiere D., Sockrider G., Morales C.. 2013. Wroldwide Infrastructure Security Report, Volume 8. Arbor Netwroks Inc. USA. Finns att laddas ner. http://www.arbornetworks.com/resources/infrastructure-security-report

Cowder T. 2008. 7 Layers of OSI. Finns att laddas ner. http://www.sis.pitt.edu/~icucart/networking_basics/7layersofOSI.htm

RieoRey Inc.. 2011. RioRey Taxonomy of DDoS Attacks. USA. Finns att laddas ner. http://www.riorey.com/x-resources/2011/RioRey_Taxonomy_DDoS_Attacks_2.2_2011.pdf

Nachreiner C.. 2013. TDoS: The latest wave of Denial of Service Attacks. Help Net Security. USA. Finns att laddas ner. http://www.net-security.org/article.php?id=1828

Arbor Networks Inc.. 2013. Quantifying the Risk of a DDoS Attack. Arbor Networks Inc.. USA. Finns att laddas ner. http://www.arbornetworks.com/resources/media-library/provider-materials

Arbor Netwroks Inc.. 2013. Peakflow Threat Management System. Arbor Networks Inc.. USA. Finns att laddas ner. http://www.arbornetworks.com/resources/media-library/provider-materials

Mötes- och konferensföredrag

Hume Duncan. 14.10.2013. RioRey företagspresentation. Vasa, Finland.

Seimann Robert. 20.9.2013. RadWare företagspresentation. Vasa, Finland.

SEKRETESSBELAGD