**Arbor Networks 13:e årliga världsomspännande infrastrukturrapport (WISR)**

**Sammandrag av rapporten**

Detta dokument innehåller ett sammandrag av resultaten från Arbor Networks 13:e årliga och världsomspännande infrastrukturrapport (WISR). Rapporten innehåller svar från nätverks- och säkerhetsansvariga hos världens ledande tjänsteleverantörer, moln-/värdtjänstleverantörer och storföretag. Den spänner över ett stort antal frågor, från hotupptäckt och incidentrespons till hanterade tjänster, bemanning och budget. Tyngdpunkten ligger på de verksamhetsmässiga utmaningar man står inför och de strategier man använder för att möta och övervinna dem.

**SLUTSATSER**

**Stora attacker mot moln- och datacenter**

Volumetriska attacker syftar till att förbruka bandbredden i ett nätverk eller en tjänst eller mellan nätverket/tjänsten och det övriga internet. Attackerna går helt enkelt ut på att orsaka överbelastning och förhindra legitima användare från att komma åt nätverk, applikationer och tjänster.

* 57 procent av storföretagen och 45 procent av datacenteroperatörerna svarade att internetbandbredden hade överbelastats på grund av distribuerade DDoS-attacker (denial-of-service).

**Attackinnovation**

IoT-botnätanvändes inte bara för högvolymattacker under 2017, utan också för att utlösa attacker mot applikationer, tjänster och infrastrukturenheter, exempelvis brandväggar. WISR-rapporten 2017 innehåller flera exempel som visar att det finns behov av ett hybridförsvar i flera nivåer som inbegriper granskning av inkommande trafik till applikationer och tjänster.

**Applikationer:** Under 2017 skedde en ökning på 30 procent av antalet storföretag som upplevde attacker i applikationslagret.

* 73 procent inriktades på HTTP.
* 69 procent inriktades på DNS.
* 68 procent inriktades på HTTPS.

**Kryptering:** Kryptering är tveklöst en nödvändig och grundläggande komponent i onlinesäkerheten. Men i takt med att fler tjänster förlitar sig på kryptering skedde också fler DDoS-attacker mot dessa tjänster under 2017.

* 53 procent av de identifierade attackerna inriktades på en krypterad tjänst i applikationslagret.
* 42 procent av de tillfrågade drabbades av attacker mot SSL/TLS-protokollet.

**Infrastruktur**: IPS-enheter, brandväggar och andra säkerhetsprodukter är nödvändiga delar av en försvarsstrategi i flera lager. Men även om de är effektiva när det gäller att stärka nätverksintegriteten och sekretessen klarar de inte av att hantera en viktig fråga i samband med DDoS-attacker: nätverkstillgänglighet. TCP-lägesutmattande attacker syftar till att förbruka de anslutningstillståndstabeller som finns i många infrastrukturkomponenter, som lastbalansering, brandväggar och själva applikationsservrarna. Lokala DDoS-skyddslösningar implementeras framför dessa enheter och skyddar dem mot attacker.

* 61 procent hade drabbats av attacker mot nätverksinfrastrukturer.
* 52 procent hade brandväggar eller IPS-enheter som slutade fungera eller bidrog till avbrott under en DDoS-attack.

**Tjänster**: Populära e-post- och VoIP-tjänster drabbades oftare av attacker under 2017, vilket tyder på att DDoS-angriparnas fokus har flyttats till att utnyttja mer sårbara tjänster.

**Mer omfattande konsekvenser**

Högprofilerade DDoS-attacker har lett till en bättre insikt om hotbilden på ledningsnivå. Under 2017 rapporterade 77 procent av de tillfrågade företagen att DDoS ingick antingen i deras verksamhetsplan eller IT-riskbedömning. Detta är en ökning på 70 procent från föregående år. En annan faktor som har fått företagsledningarna att vakna är att konsekvenserna av framgångsrika attacker har blivit allvarligare.

* Antalet organisationer som rapporterade intäktsförluster till följd av DDoS-attacker nästan fördubblades under 2017.
* 57 procent angav att skadat rykte/varumärke var den främsta konsekvensen av attackerna för verksamheten, följt av ökade driftskostnader.
* Antalet tillfrågade som rapporterade ökade kostnader för internetavbrott från 501 till 1 000 USD per minut ökade med nästan 60 procent.
* 10 procent av företagen bedömde kostnaden för en större DDoS-attack till mer än 100 000 USD under 2017, vilket är fem gånger mer än tidigare.

**Bemanningsproblem är ett ständigt hot**

Nätverks- och säkerhetsteamen är väktarna i vår uppkopplade värld, men de står inför utmaningar i form av ett aktivt och komplext hotlandskap och ständiga bemanningsproblem. Brist på resurser och svårigheter att anställa och behålla kompetent personal var återigen de två främsta problemen när det gäller att bygga upp effektiva operationella säkerhetsteam under 2017.

* 54 procent av företagen och 48 procent av tjänsteleverantörerna har problem med att anställa och behålla kompetent personal.
* 38 procent av företagen förlitar sig på tredje part och outsourcade tjänster, vilket är en ökning från 28 procent 2016. Endast 50 procent genomförde övningar i IT-försvar och andelen undersökningsdeltagare som utförde övningar minst en gång i kvartalet sjönk från 40 till 32 procent.
* En konsekvens av bemanningsproblemen är att det finns mindre tid att genomföra utbildningar i incidentrespons. Bland tjänsteleverantörerna ökade andelen som inte genomförde sådana övningar och inte heller hade några planer på att införa dem från 29 till 34 procent.
* Mindre än en fjärdedel av tjänsteleverantörerna vare sig deltog i globala operationella säkerhetsgrupper eller delade med sig av eller distribuerade observerade cybersäkerhetshot och insamlade underrättelser.

**Automatisering som den första försvarslinjen**

För tjänsteleverantörer är antalet attacker ett stort problem som har lett till ökade investeringar i teknik som automatiserar lindring av DDoS-attacker.

* 88 procent av de tillfrågade tjänsteleverantörerna använder sig av intelligenta DDoS-lindringslösningar och 36 procent använder teknik som automatiserar lindring av DDoS-attacker.
* 30 procent av tjänsteleverantörerna kan omedelbart lindra attacker med hjälp av lokala eller ständigt aktiva molntjänster.

**Undersökningens omfattning och demografi**

* Uppgifterna i 2017 års WISR-undersökning bygger på 390 svar från tjänsteleverantörer, värdtjänstleverantörer, mobiloperatörer, storföretag och andra typer av nätverksoperatörer i hela världen.
* Två tredjedelar av alla respondenter identifierade sig som yrkespersoner inom säkerhet, nätverk eller drift.
* Insamlade data innefattar november 2016 till oktober 2017.