TRAFICOM
Transport- och kommunikationsverket
Cybersäkerhetscentret

Anvisning – Överbelastningsangrepp

Traficoms forskningsrapporter och utredningar
25/2022

Innehållsförteckning

1 Inledning

1.1 Syftet med anvisningen

Denna anvisning har utarbetats av Cybersäkerhetscentret vid Transport- och kommunikationsverket Traficom och syftar till att ge organisationer råd i situationer, där man misstänker ett överbelastningsangrepp eller där ett överbelastningsangrepp hindrar den normala verksamheten. Fokus för anvisningen ligger på att behandla särdragen för denna typ av informationssäkerhetsincident. För att lösa situationen i sin helhet är det bra om organisationen upprätthåller och följer den incidenthanteringsplan som den upprättat för informationssäkerhetsincidenter (eng. Incident Response Plan).

Denna anvisning ger övergripande vägledning för hur man ska agera vid informationssäkerhetsincidenter och hur man kan återhämta sig från dem. Det rekommenderas att organisationen upprättar en egen separat guide, som på en mer detaljerad nivå beaktar organisationens tekniska och operativa miljö. Projektet har finansierats av Försörjningsberedskapscentralen.

1.2 Vad är ett överbelastningsangrepp?

Ett överbelastningsangrepp (eng. Denial of Service Attack) är ett angrepp med hjälp av vilket en illvillig aktör försöker hindra användningen av en webbresurs eller tjänst genom att störa dess funktion. Angreppet kan genomföras till exempel genom att belasta måltjänsten eller nättrafiken med extra trafik eller utnyttja en sårbarhet i en tjänst eller nätenhet. Numera är största delen av överbelastningsangreppen spridda, det vill säga trafiken skickas till målet från flera olika källor samtidigt. Bakom spridda angrepp ligger det ofta ett botnät, som angriparen kontrollerar och som består av flera enheter anslutna till internet. Enheterna har kapats för att användas i angreppet utan att enheternas ägare vet om det.

Överbelastningsangrepp sker vanligtvis genom att man antingen överbelastar målet med en stor mängd trafik eller alternativt skickar sådan trafik, som får målenheten att använda mer minnes- eller beräkningsresurser än normalt för att hantera trafiken, varvid mängden trafik inte behöver vara särskilt stor. Denna typ av angrepp visar sig inte nödvändigtvis i form av en onormalt stor trafikmängd.

Vid överbelastningsangrepp på applikationsnivå kan målet vara till exempel en databas som körs i bakgrunden och som belastas genom stora mängder förfrågningar via själva applikationen.

I dag kräver ett överbelastningsangrepp inget stort tekniskt kunnande, eftersom ett sådant kan köpas som en förmånlig tjänst på till exempel det mörka nätet. Angrepp används ofta för utpressning, ofog eller politiska påtryckningar (så kallad hacktivism), varvid den som beställt angreppet och den som utför det vanligtvis är olika aktörer.

Det finns många olika sätt att genomföra ett angrepp och alla har samma slutresultat. En klassisk metod är spridda TCP SYN-översvämningsangrepp, där ett botnät skickar stora mängder TCP SYN-paket till målet och låter bli att skicka ACK-paket. Detta leder till att målets TCP-stack fylls med halvfärdiga TCP-handskakningar, och servern eller enheten kan inte längre ta emot nya kontaktförfrågningar. I beredskapen är det bra att fokusera på bekämpning av de vanligaste angreppssätten.

2 Beredskap

Generellt är det IT-tjänsteleverantören som har ansvar för att åtgärda störningar i datatrafiken, vilket betyder att en snabb återhämtning från en störning förutsätter ett servicenivåavtal (eng. Service Level Agreement, SLA), som ålägger tjänsteleverantören att snabbt återställa servicenivån.

Vid ett överbelastningsangrepp kan ett separat avtal för att lindra konsekvenserna när angreppet inträffar vara nödvändigt. Det är även skäl att hålla nätenheternas och servrarnas programvaror uppdaterade, eftersom en del överbelastningsangrepp utnyttjar sårbarheter i programvaror.

Utöver avtalen ska man se till att dataförbindelserna är dubblerade och att det finns eventuella backupsystem, beroende på hur kritiskt systemet i fråga är. När en störning inträffar är det skäl att i förväg känna till en verksamhetsmodell, som garanterar smidig kommunikation mellan företaget och tjänsteleverantörerna samt att situationsledningen är definierad och att situationen dokumenteras. De personer som deltar i åtgärdandet av störningen ska ha tydliga roller, och utredningsprocesserna ska vara tydliga och ändamålsenliga.

Organisationen kan bedöma sin beredskap genom att använda till exempel Cybersäkerhetscentrets Cybermätare.[1] Cybersäkerhetscentret har även publicerat en separat anvisning för förebyggande och bekämpning av överbelastningsangrepp (på finska).[2]

2.1 Administrativa åtgärder

- Upprätta en incidenthanteringsplan för din organisation för användning i händelse av ett överbelastningsangrepp.
- Utbilda personalen i hur den ska agera medan en sådan incident som beskrivs i anvisningen råder.
    - Erbjud även vanliga arbetstagare en grundläggande utbildning, där de får råd för hur de ska agera om ett överbelastningsangrepp lamslår företagets tjänster.
- Ta i förväg reda på hur du kan anmäla en informationssäkerhetsincident till Cybersäkerhetscentret.[3] Följ Cybersäkerhetscentrets aktuella meddelanden.[4]
- Gå igenom olika angreppsscenarier tillsammans med ledningen och kom överens om praktiska åtgärder samt ledningsansvar och -befogenheter vid informationssäkerhetsincidenter.
- Öva på[5] och utveckla incidenthanteringsplanen regelbundet med hjälp av diskussionsbaserade övningar (eng. Tabletop Exercise), där de ansvariga personerna och intressenterna övar på processen för hantering av informationssäkerhetsincidenter i ett fiktivt scenario.
- Inför processer för kontinuerlig hantering av sårbarheter och uppdateringar.
- Identifiera de komponenter som är kritiska för affärsverksamheten samt skapa och upprätta en förteckning över de objekt som ska skyddas.
- Definiera noggrant vilka behörigheter som behövs för användarna och de tekniska funktionerna.

[1] https://www.kyberturvallisuuskeskus.fi/sv/vara-tjanster/lagesbild-och-natverksledarskap/cybermataren
[2] https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Ohje_3_2016_Palvelunestohyokkaysten_ehkaisy_ja_torjunta_0.pdf

[3] https://www.kyberturvallisuuskeskus.fi/sv/anmal
[4] https://www.kyberturvallisuuskeskus.fi/sv/ajankohtaiset
[5] https://www.kyberturvallisuuskeskus.fi/sv/vara-tjanster/ovningar

- Överväg att inrätta ett säkerhetsoperationscenter (SOC) eller att köpa en motsvarande tjänst. Syftet med en sådan säkerhetstjänst är att övervaka ditt företags nättrafik och informationssäkerhetsincidenter i systemen.

- Se till att avtalen med tjänsteleverantörerna inkluderar bekämpning av överbelastningsangrepp.

2.2 Tekniska åtgärder

- Sträva efter att upptäcka angrepp så tidigt som möjligt med hjälp av olika centraliserade monitoreringslösningar, vars funktion även testas då och då. Till exempel IDS-lösningar (eng. Intrusion Detection System) upptäcker angrepp och försöker ofta förhindra dem automatiskt.

- Håll servrarnas programvaror uppdaterade och kontrollera att konfigurationerna överensstämmer med rekommendationerna. Med rätt konfigurationer kan konsekvenserna av överbelastningsangrepp lindras.

- Konfigurationer som dämpar överbelastningsangrepp kan innehålla till exempel hastighetsbegränsningar för enskilda förbindelser (eng. Rate Limiting), förlängningar av TCP-anslutningars bearbetningsköer (eng. Backlog Queue), återanvändning av oavslutade TCP-anslutningar (eng. Half-Open Connection Recycling) eller ibruktagande av SYN-kakor (eng. SYN Cookies). Ta reda på vilka av dessa tekniker som lämpar sig bäst för er servermiljö och inför dem efter behov.

- Cybersäkerhetscentret har publicerat en teknisk guide för hur man försvarar sig vid ett överbelastningsangrepp (på finska).[6]

2.3 Beredskap och övning i praktiken

En viktig del av beredskapen är även att öva på hotscenarier. Genom att öva på scenariot i denna anvisning i förväg kan organisationen säkerställa att den är redo att möta en dylik situation. Genom att öva försäkrar sig organisationen bland annat om att personalen förstår vad punkterna i arbetsflödesschemat och checklistan i anvisningen betyder och att den har förmåga att agera enligt de anvisningar som beskrivs.

Scenariot i detta fall skulle till exempel kunna vara en situation, där ett överbelastningsangrepp lamslår ett kritiskt datasystem och helt och hållet hindrar användningen av systemet och dess funktion.

Hur skulle man i din organisation agera vid en dylik informationssäkerhetsincident? Öva på åtminstone följande steg i dessa anvisningar:
- Informera om incidenten och eskalera situationen.

- Meddela berörda tjänsteleverantörer och övriga intressenter om situationen.

- Inför ett backupsystem.

- Genomför en process för den slutliga utredningen av incidenten.

Vid sidan om alla steg att öva på är det bra att tänka på hur organisationen leder hanteringen av informationssäkerhetsincidenten, hur den interna kommunikationen fungerar samt vem som i vilket skede är ansvariga personer och vem deras ersättare är. Organisationer rekommenderas även ta del av Cybersäkerhetscentrets material om övningar.[7]

[6] https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Ohje_3_2016_liite_1_Palvelunestohyokkaysten_tekniikkaa_puolustajille_0.pdf
[7] https://www.kyberturvallisuuskeskus.fi/sv/vara-tjanster/ovningar

3 Upptäcka en informationssäkerhetsincident

Ett överbelastningsangrepp upptäcks vanligtvis när tjänsterna slutar fungera. Även genom omfattande övervakning kan ett angrepp upptäckas innan det påverkar tillgången till tjänsterna, till exempel på basis av kraftigt ökad datatrafik eller en snabb ökning av resursförbrukningen på en server. Målet för en del överbelastningsangrepp kan vara att orsaka ett fel i en enskild nätenhet, varvid det inte nödvändigtvis syns några stora förändringar i trafikmängderna. Därför är det viktigt att enskilda nätenheters funktion omfattas av övervakningen.

Anmäl informationssäkerhetsincidenten till Cybersäkerhetscentret.[8] Vi ger er konfidentiellt och kostnadsfritt råd för hur ni begränsar skadorna, analyserar incidenten och vidtar återställande åtgärder. Samtidigt stöder ni den nationella lägesbilden av informationssäkerheten och gör det möjligt för oss att varna och hjälpa andra eventuella offer.

[8] https://www.kyberturvallisuuskeskus.fi/sv/anmal

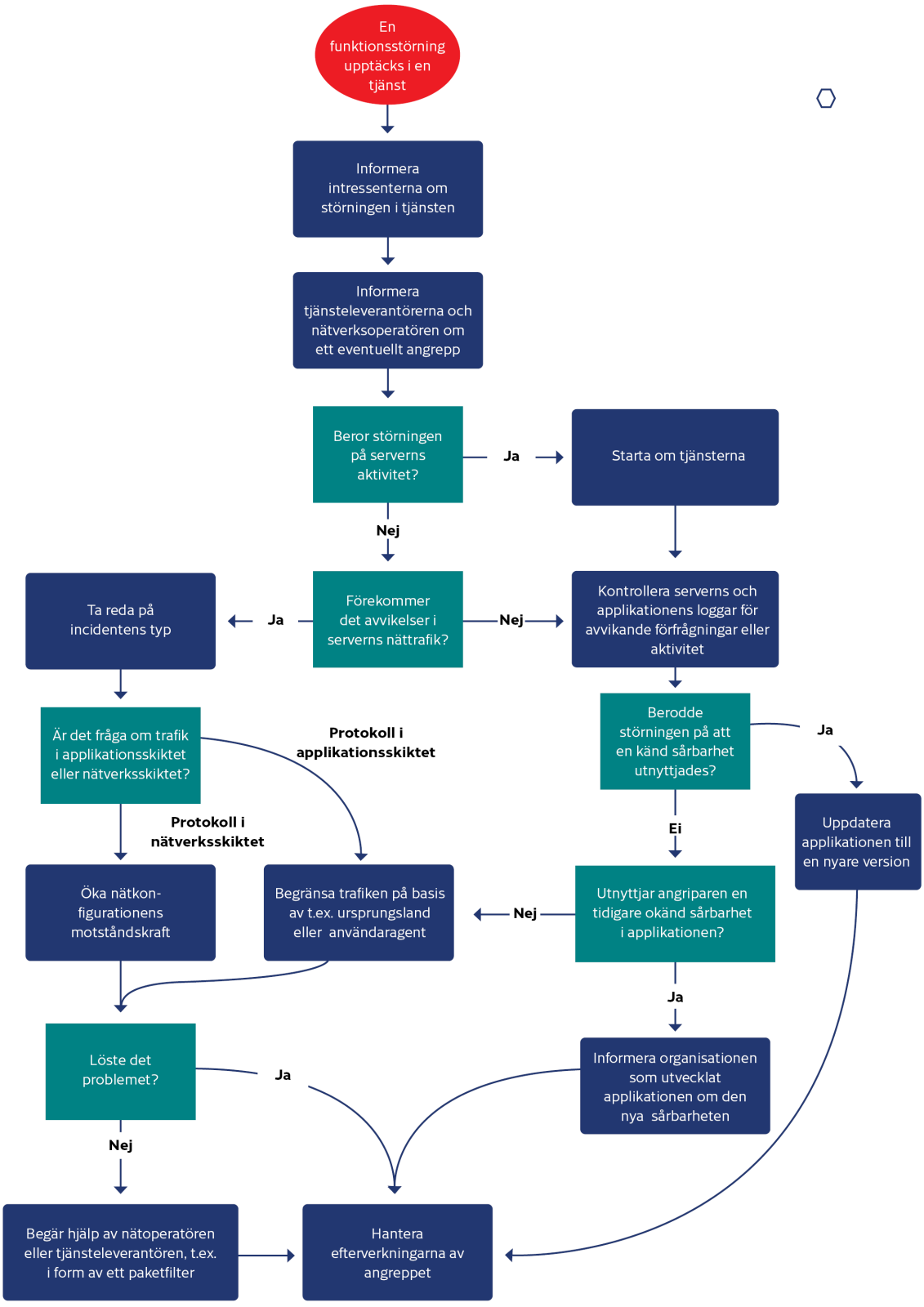
4 Anvisningar

Använd nedanstående checklista på åtgärder som hjälp när du misstänker att du fallit offer för ett överbelastningsangrepp. Checklistan hjälper din organisation att prioritera och dela in verksamheten vid utredningen av en informationssäkerhetsincident.

4.1 Arbetsflödet vid utredning av en informationssäkerhetsincident

Nedanstående flödesplan beskriver de åtgärder som ska tillämpas för att en incident ska kunna utredas i rätt ordning. Flödesplanen stöder användningen av checklistan. Under utredningen är det även ytterst viktigt att föra en noggrann händelselogg över de åtgärder som vidtagits. Av loggen ska framgå vilken åtgärd som genomförts, tidsstämpeln för den och vem som utfört åtgärden.

Det är även skäl att omsorgsfullt dokumentera eventuellt bevismaterial. Det bör antecknas vem som samlat in materialet, vad materialet består av samt var och när det har samlats in. En omsorgsfullt upprättad händelselogg underlättar avsevärt utredningen samt samarbetet med polisen och datasäkerhetsforskarna.


En funktionsstörning upptäcks i en tjänst
Informera intressenterna om störningen i tjänsten
Informera tjänsteleverantörerna och nätverksoperatören om ett eventuellt angrepp
Beror störningen på serverns aktivitet?
Ja
Starta om tjänsterna
Nej
Ta reda på incidentens typ
Ja
Förekommer det avvikelser i serverns nättrafik?
Nej
Kontrollera serverns och applikationens loggar för avvikande förfrågningar eller aktivitet
Är det fråga om trafik i applikationsskiktet eller nätverksskiktet?
Protokoll i applikationsskiktet
Protokoll i nätverksskiktet
Berodde störningen på att en känd sårbarhet utnyttjades?
Ja
Ei
Uppdatera applikationen till en nyare version
Öka nätkon-figurationens motståndskraft
Begränsa trafiken på basis av t.ex. ursprungsland eller användaragent
Nej
Utnyttjar angriparen en tidigare okänd sårbarhet i applikationen?
Ja
Löste det problemet?
Ja
Informera organisationen som utvecklat applikationen om den nya sårbarheten
Nej
Begär hjälp av nätoperatören eller tjänsteleverantören, t.ex. i form av ett paketfilter
Hantera efterverkningarna av angreppet

4.2 Omedelbara åtgärder

Stegets mål	Det är viktigt att åtgärderna är både exakta och snabba. Målet med de omedelbara åtgärderna är att begränsa orsaken till störningen i datakommunikationen och att så snabbt som möjligt inleda lindrande eller korrigerande åtgärder.

Steg	Syfte	Åtgärder
Kontrollera läget i servrarna för den tjänst som är föremål för störningen	Målet är att avgränsa orsaken till störningen så exakt som möjligt. Om det till exempel förekommer en störning på en webbplats kan orsaken vara en felsituation i någon av servrarna bakom webbplatsen. Även ett överbelastningsangrepp kan leda till att en bakgrundsapplikation kraschar.	Be administratören av applikationsservern att kontrollera applikationens status och loggar samt serverns resursanvändning. Om det finns bakgrundstjänster, till exempel databaser, i anslutning till applikationen ska även dessa kontrolleras separat.
Kontrollera eventuella avvikelser i trafiken för den tjänst som är föremål för störningen och identifiera angreppets typ	Ett överbelastningsangrepp syns i många fall i form av en kraftigt ökad trafikmängd. Därför kan en ökad trafikmängd i kombination med en tjänst som inte fungerar vara ett tecken på ett överbelastningsangrepp. Det är även viktigt att identifiera överbelastningsangreppets typ för att underlätta bekämpningen.	Kontrollera om det har kommit fler förfrågningar än normalt i applikationens loggar och varifrån förfrågningarna kommer. En plötslig ökning av mängden förfrågningar från till exempel utländska IP-adresser kan vara ett tecken på ett överbelastningsangrepp. Största delen av överbelastningsangreppen görs i dag i form av TCP SYN-översvämningsangrepp. Dessa angrepp är svårare att upptäcka, eftersom de inte syns i webbserverns loggar. De kan dock upptäckas i realtid i form av en onormalt stor mängd SYN RECV-rader i servrarnas TCP-anslutningslistor. Ett angrepp på applikationsnivå syns i allmänhet i form av ovanliga HTTP-förfrågningar i webbserverns loggar eller alternativt i form av normala förfrågningar, som det finns exceptionellt många av. Denna typ av angrepp är tekniskt sett enklast att genomföra, men orsakar även minst skada på målet. Ett förstärkt DNS-angrepp syns även i form av ett ökat antal HTTP-förfrågningar i loggarna, men orsakar betydligt mer skada jämfört med ett vanligt HTTP-angrepp på applikationsnivå. Angriparen genomför det genom att skicka DNS-förfrågningar, vars avsändaradress har förfalskats så att de ser ut att komma från den organisation som är föremål för angreppet, till flera namnservrar. Då skickar servrarna ett svar tillbaka till målet för angreppet och överbelastar det. Ett angrepp kan kännas igen i loggarna i form av HTTP-svar utan någon motsvarande förfrågan.

Kontakta din IT-/IKT-tjänsteleverantör	Ofta har en del av organisationers IT-infrastruktur utkontrakterats till en tjänsteleverantör. Skadlig trafik går nästan alltid via tjänsteleverantörens nätverk, varvid denna har möjlighet att filtrera trafiken om man har avtalat om det i förväg.	Gör en anmälan om incidenten till din IT- eller IKT-tjänsteleverantör, beroende på vilken tjänst som är föremål för angreppet. Om angreppet är ett så kallat volumetriskt angrepp, det vill säga det baserar sig på en stor mängd trafik, kan tjänsteleverantören hjälpa till att stoppa angreppet genom att begränsa trafiken till tjänsten med hjälp av ett paketfilter.
Informera de samarbetspartner och intressenter som kan påverkas om informationssäkerhetsincidenten	Incidenten kan leda till risker eller problem med tillgången till tjänster för samarbetspartner, kunder och tjänsteleverantörer.	Informera intressenternas kontaktpersoner vid krissituationer om incidenten om du tror att den kan påverka tillgången till deras tjänster. Informera även internt om incidenten, i synnerhet om angreppet även begränsar tillgången till interna tjänster.
Bedöm om du behöver utomstående hjälp för att hantera incidenten	Organisationen kan behöva hjälp med de tekniska åtgärderna, hanteringen av incidenten och organiseringen av åtgärderna. Om det inte finns tillräcklig kompetens internt eller hos de IT-tjänsteleverantörer som anlitas ska man överväga att anlita hjälp utifrån.	De tekniska åtgärderna vid hanteringen av en incident kan kräva extern kompetens. Sådana åtgärder kan vara bland annat insamling av identifieringsuppgifter och utredning av hotet utifrån dem. Cybersäkerhetscentret kan hjälpa organisationer med i synnerhet de första insatserna och genom att erbjuda tilläggsinformation om liknande fall i Finland och internationellt. I resurserna i fotnoten hittar du finländska tjänsteleverantörer.[9]
Rapportera informationssäkerhetsincidenten till myndigheterna	Rapportera incidenten till myndigheterna. Organisationen kan enligt författningar eller en cyberförsäkring vara skyldig att anmäla incidenten.	Gör en brottsanmälan om händelsen till polisen.[10] Anmäl händelsen även till Cybersäkerhetscentret[11] för att upprätthålla lägesbilden och få hjälp. Aktörer och tjänsteleverantörer som är kritiska med tanke på försörjningsberedskapen ska rapportera informationssäkerhetsincidenter i sina nätverks- och datasystem till myndigheterna.[12]

[9] https://dfir.fi/
https://www.fisc.fi/fi
https://www.hansel.fi/sv/upphandlingar/tiedonhallinnan-ja-digiturvallisuuden-asiantuntija/

[10] https://poliisi.fi/sv/gor-en-brottsanmalan

[11] https://www.kyberturvallisuuskeskus.fi/sv/anmal

[12] https://www.kyberturvallisuuskeskus.fi/sv/vara-tjanster/rapportera-en-it-sakerhetsincident-nis-skyldighet

4.3 Utredning av en informationssäkerhetsincident

Stegets mål	Målet med att utreda incidenten är att klarlägga på vilket sätt angreppet har orsakat en störning i tjänsten och genom det få information om hur man framöver kan skydda sig mot liknande angrepp.

Steg	Syfte	Åtgärder
Ta reda på vilka målen för angreppet har varit	Det är viktigt att identifiera vilken del av infrastrukturen som var målet för överbelastningsangreppet. Om det till exempel gäller en webbtjänst är det viktigt att ta reda på huruvida angreppet till exempel var riktat direkt mot webbplatsens server eller mot nätenheter i anslutning till den.	Kontrollera loggdata för den server som var föremål för angreppet. Om det är fråga om en webbplatsserver kan angreppet synas i form av ett ökat antal förfrågningar i loggarna. Om det handlar om ett TCP SYN-översvämningsangrepp eller något annat angrepp mot ett lägre protokoll kan det vara svårt att utreda utan IT-tjänsteleverantörens hjälp.
Ta reda på angreppets typ	Det är viktigt att ta reda på vilken typ av angrepp det är fråga om, så att tjänsten kan skyddas bättre framöver. Det kan vara fråga om ett angrepp mot ett applikationsskikt, såsom HTTP, eller ett nätverksskikt, såsom TCP, eller så kan angriparen ha utnyttjat en sårbarhet i en programvara.	Om angreppet har genomförts genom att utnyttja en sårbarhet i målsystemet ska det uppdateras för att åtgärda sårbarheten. Om det handlar om en applikation som organisationen beställt någon annanstans ifrån ska man för att åtgärda sårbarheten kontakta den aktör som levererat applikationen. Vid volymetriska angrepp är det effektivaste sättet att försvara sig att IT- eller IKT-tjänsteleverantören filtrerar trafiken, vilket kräver separata avtal med tjänsteleverantören. Angrepp mot ett protokoll i ett applikationsskikt, det vill säga angrepp på applikationsnivå, kan man försöka bekämpa på egen hand, till exempel genom att begränsa förfrågningarna utifrån IP-adress, domännamn, webbläsarens användaragent eller IP-adressens geoplats.
Spara alla loggar med anknytning till incidenten för senare undersökning	Syftet med att samla in och spara bevis är att säkerställa en högklassig utredning av incidenten i efterhand, så att grundorsakerna till den kan klarläggas. Bevisen kan behövas i samband med en brottsutredning och för en rättsprocess.	Spara alla loggfiler som innehåller viktig information med tanke på utredningen av incidenten på den hårddisk som isolerats från nätverket.

4.4 Återställande

Stegets mål	Överbelastningsangrepp pågår i medeltal i mindre än 15 minuter, men ibland kan de pågå i flera timmar. Efter angreppet återgår tjänsterna i allmänhet till normal funktion av sig själva.

Steg	Syfte	Åtgärder
Kontrollera de delar av tjänsten som var föremål för angreppet för eventuella felsituationer	Överbelastningsangreppet kan ha fått den server eller nätenhet som var målet att hamna i felläge, varvid det är bra att kontrollera att servrarna och de applikationer som körs på den fungerar normalt.	Kontrollera statusen för de servrar och nätenheter som var målet för angreppet. Kontrollera även att applikationerna fungerar normalt.
Kontrollera att servrarnas programvaror och konfiguration är uppdaterade	I överbelastningsangreppet kan angriparen ha utnyttjat en sårbarhet i en applikation eller en server, så det är skäl att kontrollera att servern är uppdaterad.	Gå igenom applikationsversionerna på den server som var målet för angreppet och uppdatera vid behov till den senaste. Undersök i applikationens loggar hurdana förfrågningar applikationen har tagit emot för att få reda på vilka förfrågningar som kan ha utnyttjats som en del av angreppet.

5 Efterverkningar av informationssäkerhetsincidenten

När krisen är över och affärsfunktionerna normaliserat sig är det viktigt att börja hantera efterverkningarna av angreppet och lära sig av det inträffade för framtiden. Samtidigt är det skäl att uppdatera krishanteringsplanerna utifrån de observationer som gjorts. Det är möjligt att organisationen på nytt faller offer för ett liknande angrepp om grundorsakerna till det inträffade inte kommer fram och man inte tar lärdom av händelsen.

Vid hanteringen av efterverkningarna (eng. Post-Incident Review) granskas verksamheten i krissituationen: vilka åtgärder genomfördes väl, var fanns det utrymme för förbättringar samt hur kan säkerhetsnivån och -planerna förbättras? Det är skäl att utarbeta en rapport om hanteringen av efterverkningarna som, förutom händelseförloppet, även inkluderar svar på åtminstone följande frågor:

- Grundorsaker till incidenten:
    - Vilka tekniska eller funktionsmässiga svagheter ledde till situationen?
- Det egna skyddets effektivitet:
    - Var de kontroller som användes för att upptäcka angrepp tillräckliga?
    - Orsakade angriparens handlingar några larm?
    - Hur reagerade man på larmen? Fick rätt ansvariga personer information om larmen?
- Agerande i krissituationen:
    - Följde man krisplanen? Hur användbar var den?
    - Fördelades krisgruppens ansvar mellan rätt personer?
    - Hur väl lyckades man begränsa angreppet och driva bort angriparen?
    - Hur väl lyckades krisgruppens kommunikation? Hur beaktades intressenterna?
- Återställande:
    - Hur väl lyckades man återställa kritiska uppgifter och tjänster?
- Efterverkningar:
    - Har händelseförloppet och utredningsarbetet dokumenterats?
    - Var den tekniska utredningen av incidenten tillräcklig? Har man kunnat förse till exempel myndigheterna med tillräckligt med material om angreppet?
    - Utvärdera tjänsteleverantörernas verksamhet. Var svarstiden och de avtalade tjänsterna tillräckliga för att utreda incidenten?

Efter incidenten ska organisationen uppdatera sin incidenthanteringsplan och sina mer detaljerade anvisningar för bekämpning av olika typer av avvikelser. Det rekommenderas även att organisationerna med jämna mellanrum övar på olika scenarier, så att nyttan med dem kan garanteras vid en krissituation.

Cybersäkerhetscentret önskar att företag och organisationer skulle dela med sig av de viktigaste lärdomarna som de dragit av incidenter. Med hjälp av fallrapporter kan Cybersäkerhetscentret hjälpa andra organisationer i Finland och utomlands vid utredningen av liknande fall. De lärdomar som återställandet ger bidrar till att utveckla beredskapen för alla organisationer.

Transport- och kommunikationsverket Traficom
Cybersäkerhetscentret
PB 320, 00059 TRAFICOM
tfn 029 534 5000

kyberturvallisuuskeskus.fi

ISBN 978-952-311-817-1

FÖRSÖRJNINGS-
BEREDSKAPCENTRALEN

TRAFICOM
Transport- och kommunikationsverket
Cybersäkerhetscentret