NATIONELLT CYBERSÄKERHETSCENTER

Överbelastningsangrepp mot kritisk infrastruktur i Norden och Baltikum hösten 2024

Tillvägagångssätt, infrastruktur och rekommendationer

Mars 2025

Innehåll

Sammanfattning

— De senaste två åren har överbelastningsangrepp mot olika verksamheter blivit vanligare och också ökat i intensitet. Samtidigt har verktyg för att genomföra överbelastningsangrepp blivit tillgängliga för fler aktörer.

— Överbelastningsangrepp med geopolitiska motiv har ökat mot kritisk infrastruktur i både Europa och Sverige. Under hösten 2024 utsattes kritisk infrastruktur i Norden och Baltikum för omfattande överbelastningsangrepp.

— En undersökning av data kopplade till dessa överbelastningsangrepp visar att nästan en tredjedel av samtliga observerade överbelastningsangrepp mot den svenska IP-rymden identifierades som kritisk infrastruktur.

— Undersökningen pekar på att botnätet Gorilla användes som infrastruktur för att genomföra dessa angrepp. Det har använts vid angrepp mot akademiska institutioner, statliga myndigheter samt mot sektorerna telekommunikation och finans i över 100 länder.

— Botnätet Gorilla har en omfattande infrastruktur som finns i ett stort antal länder. Enheterna som ingår i nätverket utgörs av en varierande uppsättning enheter, exempelvis högkapacitetsroutrar för användning i driftsmiljöer, routrar, IP-kameror, digitala videoinspelningsenheter, sårbara servrar och enheter som är en del av sakernas internet (eng. *Internet of Things, IoT).* Olika delar av infrastrukturen har distinkta funktioner och i flera delar används tekniker för att försvåra nedtagning och spårning.

— Vid angreppen mot kritisk infrastruktur i Norden och Baltikum som ingick i undersökningen användes flera olika tillvägagångssätt. Vanligast förekommande var DNS-förstärkning, IP-fragmentering samt översvämning av UPD-, TCP ACK- och TCP SYN-trafik.

— Åtgärder som rekommenderas för att mildra effekterna av liknande angrepp är bland andra att ta hjälp av internetleverantören, implementera en så kallad webbapplikationsbrandvägg (WAF), använda innehållsleveransnätverk (CDN), använda flera tjänsteleverantörer och tes ta incidenthanteringsplanen för överbelastningsangrepp.

— Rapporten är ett resultat av samarbete mellan NCSC-SE, drabbade sektorer och näringslivet.

Bakgrund

Under hösten 2024 utsattes kritisk infrastruktur i Norden och Baltikum för omfattande överbelastningsangrepp. Den utredning som ligger till grund för den här rapporten har analyserat data med koppling till dessa angrepp. Angreppen som ingår i utredningen inträffade under september och oktober. Syftet med rapporten är att skapa insikter som kan användas av både drabbade verksamheter och andra verksamheter för att öka sin motståndskraft mot liknande framtida angrepp. Rapporten är ett resultat av samarbete mellan NCSC-SE, drabbade sektorer och näringslivet.

Överbelastningsangrepp syftar till att rikta stora mängder nätverkstrafik mot en e-tjänst, en server eller ett nätverk och på så sätt göra den långsam eller otillgänglig för dess användare[1]. De senaste två åren har överbelastningsangrepp mot olika typer av verksamheter blivit vanligare och också ökat i intensitet[2].

Samtidigt har verktyg för att genomföra överbelastningsangrepp blivit tillgängliga för fler aktörer[3]. Verktygen erbjuds i vissa fall som tjänster (eng. *DDoS-as-a-Service, DDoSaaS)* där angripare mot en avgift tillfälligt får tillgång till verktyg och infrastruktur för att genomföra överbelastningsangrepp mot valfria mål. Verktygen har gjort det möjligt att anpassa tillvägagångssätt i högre grad och göra angreppen mindre förutsägbara(4).

Överbelastningsangrepp mot kritisk infrastruktur

Under 2024 ökade antalet angrepp mot kritisk infrastruktur, sannolikt drivet av geopolitiska konflikter, hacktivism och framväxten av mer avancerade tillvägagångssätt[5]. Överbelastningsangrepp med geopolitiska motiv har ökat mot kritisk infrastruktur i både Europa och Sverige[6]. Även om överbelastningsangrepp i regel har begränsad och kortvarig påverkan på de drabbade verksamheterna, kan återkommande och ihållande angrepp mot kritisk infrastruktur på sikt påverka förtroendet för dessa verksamheter.

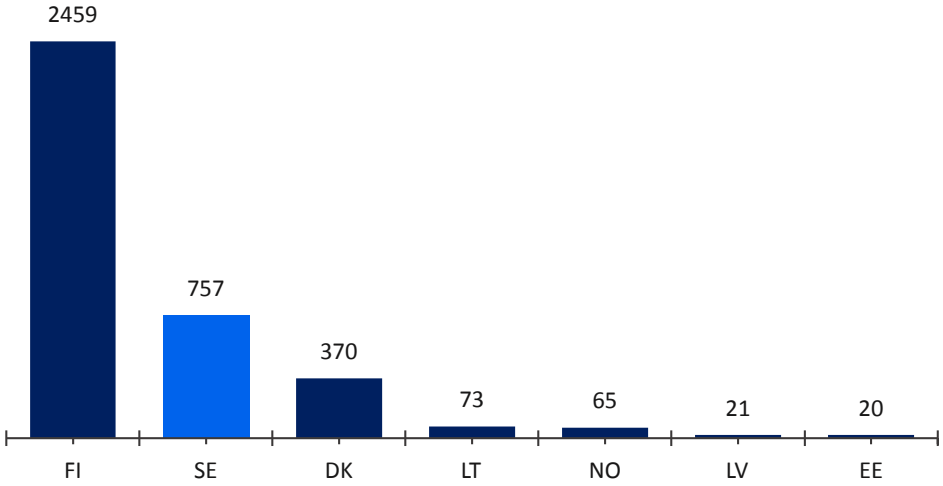
I angrepp mot kritisk infrastruktur har överbelastningsangrepp mot både nätverks- eller transportlagret (lager 3/4) och applikationslagret (lager 7) ökat. De senare har ökat avsevärt under 2024 i observerade angrepp mot verksamheter i Mellanöstern och Europa[7][8][9].

1 https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/
2 https://blog.ovhcloud.com/the-rise-of-packet-rate-attacks-when-core-routers-turn-evil/
3 Ibid.
4 https://www.akamai.com/resources/state-of-the-internet/securing-apps-report-2024
5 https://www.f5.com/labs/articles/threat-intelligence/2024-ddos-attack-trends
6 https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf
7 https://ir.netscout.com/investors/press-releases/press-release-details/2024/DDoS-Attacks-Skyrocket-and-Hacktivist-Activity-Surges-Threatening-Critical-Global-Infrastructure-According-to-NETSCOUTs-1H2024-Threat-Intelligence-Report/default.aspx
8 https://www.nasdaq.com/press-release/akamai-finds-geopolitical-tensions-driving-surge-ddos-attacks-financial-institutions
9 https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf

Överbelastningsangrepp mot kritisk infrastruktur Norden och Baltikum hösten 2024

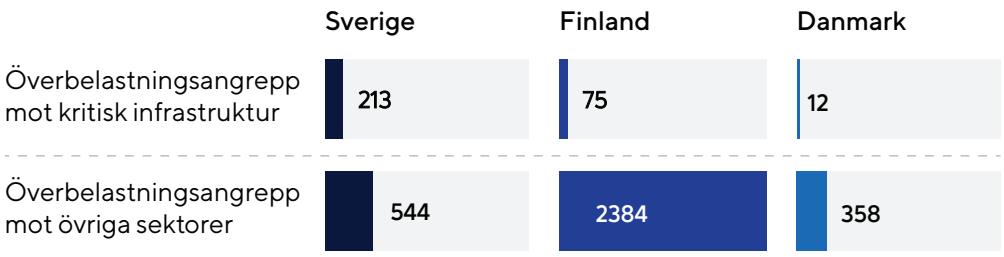
Under hösten 2024 utsattes kritisk infrastruktur i Norden och Baltikum för omfattande överbelastningsangrepp. Data med koppling till dessa angrepp har analyserats i den utredning som ligger till grund för denna rapport. Angreppen som ingår i undersökningen inträffade under september och oktober.

Figur 1. Överbelastningsangrepp mot Norden och Baltikum. Observerade i data från september och oktober 2024.



Ser man till Norden och Baltikum som helhet så identifierades cirka 3 765 mål för överbelastningsangrepp under perioden där två tredjedelar hörde till den finska IP-rymden. Ser man istället till mål som identifierades som kritisk infrastruktur var Sverige utsatt i högre grad relativt sett. Av de 757 överbelastningsangrepp som riktades mot mål i den svenska IP-rymden utgjordes nästan en tredjedel av kritisk infrastruktur. Motsvarande siffra i Finland var endast tre procent.

Figur 2. Andel överbelastningsangrepp mot kritisk infrastruktur mot verksamheter i den svenska, finska och danska IP-rymden jämfört med övriga sektorer. Observerade i data från september och oktober 2024.



I undersökningen observerades ett mönster där angriparna till synes riktar sig mot olika länders IP-rymd i sekvens snarare än parallellt. Samma mönster observerades när det gällde hur angriparna riktade sig mot individuella mål.

Vid angreppen använde sig angriparna av både volymetriska angrepp som karaktäriseras av stora mängder trafik mätt i bitar per sekund (bps) och datapaket per sekund (pps) samt av distribuerade angrepp där trafik riktas mot ett stort antal IP-adresser i den drabbade verksamheten. Exempel på påverkan i form av trafikmängd uppgick till upp till cirka 5 Mpps av TCP SYN-trafik under en period i september.

Tabell 1. Vanligt förekommande tillvägagångssätt observerade i data från undersökningen.

Tillvägagångssätt	Förekomst	Beskrivning
DNS-förstärkning	Mycket vanlig	DNS-förstärkning (eng. *DNS amplification)* innebär att angriparen skickar litet anrop till öppna DNS-tjänster från en förfalskad IP-adress som matchar målsystemet. DNS-tjänsten svarar målsystemet med ett större anrop. Flera DNS-tjänster kan anropas parallellt vilket ökar angreppets intensitet.
IP-fragmentering	Vanlig	IP-fragmentering (eng. *IP fragmentation)* innebär att angriparen skickar datapaket i fel ordning till målsystemet som i onödan tvingas använda systemresurser för att sammanfoga dem i rätt ordning.
UDP-översvämning	Vanlig	UDP-översvämning (eng. *UDP flood*) innebär att angriparen skickar ett stort antal UDP-paket till slumpmässiga portar på målsystemet som förmås svara på anropen med information om att målet inte kan nås.
TCP ACK-översvämning	Vanlig	TCP ACK-översvämning (eng. *TCP ACK flood*) innebär att angriparen skickar ett stort antal datapaket som hör till den handskakning som sker när kommunikation upprättas via TCP-protokollet. TCP-ACK är det sista steget i handskakningen och målsystemet tvingas använda systemresurser för att hantera felaktiga handskakningar.
TCP SYN-översvämning	Vanlig	TCP SYN-översvämning (eng. *TCP SYN flood*) innebär att angriparen skickar ett stort antal datapaket som hör till den handskakning som sker när kommunikation upprättas via TCP-protokollet. TCP-SYN är det första steget i handskakningen. Angriparen undviker att slutföra handskakningen vilket leder till att målsystemet tvingas använda systemresurser för att vänta på svar som inte kommer.

Botnätet Gorilla – angriparnas infrastruktur

Utredningen av överbelastningsangreppen mot kritisk infrastruktur i Norden och Baltikum hösten 2024 pekar på att botnätet Gorilla var aktivt vid angreppen.

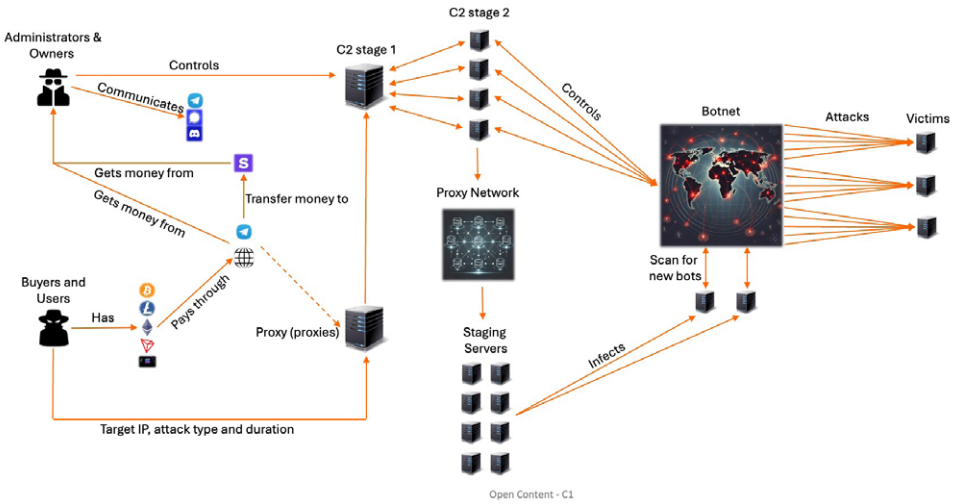
Botnätet Gorilla är en utvecklad version av botnätet Mirai. Gorilla observerades vid över 300 000 överbelastningsangrepp globalt under en och samma månad 2024[10][11]. Det har använts vid angrepp mot akademiska institutioner, statliga myndigheter samt mot sektorerna telekommunikation och finans i över 100 länder[12].

Gorilla stödjer fler processorarkitekturer än Mirai vilket gör att fler typer av enheter kan kompromitteras och göras till en del av botnätet. Det erbjuder angriparna flera olika tillvägagångssätt som kan anpassas för att kringgå den drabbade verksamhetens skyddsåtgärder[13].

Infrastrukturens uppbyggnad

Botnätet Gorilla har en omfattande infrastruktur som finns i ett stort antal länder. Olika delar av infrastrukturen har distinkta funktioner. Gorillas infrastruktur utgörs primärt av C2 kommandoservrar (eng. *command and control, C2)* som administratörerna använder för att styra botnätet, C2-servrar som används för att kontrollera noderna i botnätet, stagingservrar (eng. *staging servers*) som lagrar och sprider den skadliga programvaran som laddas ner till kompromitterade enheter samt de enskilda noderna som utgör själva botnätet. Administratörerna för botnätet Gorilla driftar ett flertal servrar, varav vissa är placerade i länder som försvårar nedtagning av västerländska myndigheter.

Figur 3. Översikt över infrastrukturen bakom botnätet Gorilla.



10 https://thehackernews.com/2024/10/new-gorilla-botnet-launches-over-300000.html
11 https://nsfocusglobal.com/over-300000-gorillabot-the-new-king-of-ddos-attacks/
12 Ibid.
13 Ibid.

När den skadliga programvaran kan exekvera kod på den komprometterade enheten, försöker den hämta installationsskript. Dessa skript stegar igenom installationsfiler till dess att den hittar en som är kompatibel med den aktuella enheten och startar sedan installationen. Att den skadliga programvaran som används i Gorilla har stöd för ett så stort antal olika processorarkitekturer gör att den kan infektera många olika typer av enheter.

Vid tillfället då utredningen avslutades observerades fem C2-servrar och en C2 kommandoserver inom botnätet. Dessa servrar är avgörande för att hantera olika uppgifter kopplade till driften av botnätet, inklusive att bearbeta data och utföra kommandon. De indikerar att botnätets infrastruktur har möjlighet att hantera många parallella anrop vilket bidrar till att öka kapacitet och driftsäkerhet. De enskilda enheter som ingår i nätverket utgörs av en varierande uppsättning enheter, exempelvis högkapacitetsroutrar för användning i driftsmiljöer, routrar, IP-kameror, digitala videoinspelningsenheter, sårbara servrar och enheter som är en del av sakernas internet (eng. *Internet of Things, IoT*). Enheterna är utspridda över hela världen inklusive i Sverige. Enheternas sammansättning ger nätverkets administratörer tillgång till en blandning av robust, professionell hårdvara och ett mycket stort antal konsumentenheter över hela världen för att öka effektiviteten i angreppen som utförs med hjälp av botnätet.

Kommunikationen mellan botnätets kontrollservrar och de stagingservrar sker via ett proxynätverk. Det gör det svårare att spåra trafiken till dess fysiska platser om någon skulle skaffa sig tillgång till enheter på nätverket. Det skapar ett anonymiseringslager mellan de som driver botnätet och de som använder det som infrastruktur för att genomföra angrepp.

Enheter och operativsystem som stöds

Baserat på analys av installationsskript och förkompilerad kod, riktar Gorilla in sig på olika distributioner av Linux (stöd finns för ARM-, MIPS- och x86-arkitektur):

ARM-arkitekturer	MIPS-arkitekturer	x86-arkitekturer	Andra arkitekturer som stöds
ARMv5	MIPSEL	x86_64 (x64)	m68k
ARMv6	MIPS	x86_32	PowerPC
ARMv7			SPARC

Tekniker för att bevara fotfäste och undvika upptäckt

Gorilla säkerställer fotfäste på komprometterade system genom att lägga till automatisk körning av script under uppstart eller inloggning, vilket gör det svårt att upptäcka och rensa bort den skadliga koden. Utöver det så använder Gorilla tillvägagångssätt för att undvika upptäckt, exempelvis genom att undersöka om enheten är en honungsfälla som ofta används för att fånga tidiga försök till intrång och spridning av skadlig programvara. Den skadliga programvaran kontrollerar om programvaror för att analysera skadlig kod är installerade på enheten.

Den skadliga programvaran använder vanligt förekommande och läckta lösenord för ett stort antal typer av IoT-enheter för att försöka infektera och sprida sig till andra enheter. Historiskt har den skadliga programvaran även utnyttjat sårbarheter för att infektera andra enheter, men det observerades inte i den senaste versionen.

Användargränssnitt

En undersökning av de kommunikationskanaler som Gorillas påstådda ägare och administratörer använder sig av, visar att botnätet har kundrelaterade tjänster som inkluderar interaktiva chattbotar på Telegram. Kunder kan använda chattbotarna för att köpa tillgång till olika tjänster som Gorilla erbjuder. Potentiella kunder kan köpa tillgång till botnätet tillfälligt eller i abonnemangslika former.

Löpande utveckling

Enligt de påstådda administratörerna för botnätet Gorilla har det löpande uppgraderats och utvecklats under de senaste månaderna för att förbättra prestanda och driftsäkerhet.

Tabell 2. Versioner och relaterade förbättringar kommunicerade från Gorillas administratörer.

Version	Påstådda förbättringar	Datum
1.4	Förbättringar av tillförlitlighet i trafikhantering samt optimeringar av stöd för molntjänster för snabbare bearbetning av förfrågningar.	Juli 2024
4	Routing- och kapacitetsproblem lösta och ytterligare servrar har lagts till för ökad stabilitet och genomflöde. Stöd för olika kommunikationsprotokoll har förbättrats, särskilt för spelapplikationer.	Oktober 2024
5 och 6	En omfattande omarbetning av funktioner på transport- och applikationslagret.	November 2024

Rekommenderande åtgärder

Många av råden nedan är hämtade från NCSC-SE:s vägledning om överbelastningsangrepp som du hittar på ncsc.se. I vägledningen finns mer detaljerade beskrivningar av bakgrunden till råden. CERT-SE, Sveriges nationella CSIRT, erbjuder råd och stöd för verksamheter som arbetar med att förebygga eller som drabbats av överbelastningsangrepp. Mer information och kontaktuppgifter finns på cert.se.

Ta hjälp av internetleverantören

— Inled och upprätthåll dialog med internetleverantören för att hålla dem uppdaterade om förändringar i er infrastruktur som kan påverka exponering och risken för överbelastningsangrepp.

— Implementera ”packet scrubbing” och andra avancerade filtreringsverktyg från internetleverantören för att effektivt filtrera och hantera skadlig trafik.

- Förstå vilka skydd leverantören kan erbjuda på högre nätverksnivåer. Notera att det kan vara svårt för leverantören att fullt ut skydda applikationer som använder krypterade protokoll (t.ex. HTTPS och TLS).

- Diskutera med internetleverantören möjligheten till geoblockering eller trafikbegränsning för specifika regioner eller nätägare som inte behöver full åtkomst, och stryp bandbredd för källor med högre risk

Implementera webbapplikationsbrandvägg (WAF)

- Installera en WAF för att skydda applikationslagret och blockera skadlig trafik innan den når applikationen.

- Identifiera och blockera mönster som tyder på angrepp, som högfrekventa anrop till resurskrävande funktioner.

- Begränsa åtkomst till sårbara URL:er för att minska risken för angrepp.

- Anpassa regler baserat på trafikmönster och hotbilder för att bibehålla ett effektivt skydd.

Använd innehållsleveransnätverk (CDN)

- Cachelagra och distribuera statiskt innehåll globalt.

- Maskera ursprungsservern och säkerställ att all trafik går genom CDN för att förhindra direkta angrepp.

- Begränsa bandbredd och åtkomst för specifika regioner eller nätägare med hög risk.

- Vid val av CDN, prioritera leverantörer med höga säkerhetskrav, lastbalansering och redundanta nätverksvägar för att hantera stora trafiktoppar.

Använd flera tjänsteleverantörer

- Öka tillgängligheten och minska sårbarheten för överbelastningsangrepp genom att använda flera tjänsteleverantörer för kritiska funktioner som DNS och nätverksanslutningar.

- Undvik leverantörer som delar resurser, som huvudnätverk eller datacenter, för att minimera risken för kedjeeffekter vid angrepp.

- Säkerställ att leverantörerna är geografiskt diversifierade för att öka redundansen och minska risken vid riktade angrepp.

- Testa din incidenthanteringsplan för överbelastningsangrepp

- Genomför regelbundna tester av åtgärderna i incidenthanteringsplanen för att förstå vilka typer och volymer av angrepp som kan hanteras och identifiera områden där ytterligare förstärkningar krävs.

- Inkludera både nätverks- och applikationslager i testerna för att säkerställa att samtliga delar av systemet är förberedda för överbelastningsangrepp.

- Använd pålitliga testleverantörer för att genomföra kontrollerade tester utan att orsaka oavsiktliga störningar.

- Implementera realtidsövervakning av nätverk, beräkningskapacitet och lagring för att analysera resursanvändning både under tester och vid faktiska angrepp.

- Använd verktyg som övervakar tillgängligheten från geografiskt spridda platser för webbaserade tjänster för att identifiera regionrelaterade sårbarheter.

- Dra nytta av övervakningsflöden och varningar från leverantörer för att få tidig insikt om trafikmönster och potentiella angrepp innan de når organisationens nätverk.

Koordinering och samverkan

Effektiv hantering av överbelastningsangrepp kräver nära och tät dialog med berörda leverantörer. Ovan berördes vikten av att ha nära dialog med internetleverantören, men verksamheten behöver upprätta effektiva kommunikationsvägar med leverantörer av CDN och överbelastningsskydd. Även samverkan med ansvariga myndigheter, betrodda leverantörer av hotinformation och andra verksamheter inom samma sektor stärker möjligheterna att hantera överbelastningsangrepp då de kan dela relevanta insikter, tidiga varningar och sektorsspecifik bäst praxis. En proaktiv hållning inom sektorer och branscher bidrar till att rätta vanligt förekommande sårbarheter och att anpassa skyddet till trender och tillvägagångssätt som är sektorsspecifik.

Försvar på kort och lång sikt

För att möta omedelbara hot behöver verksamheter optimera existerande resurser, förfina incidenthantering genom övning och säkerställa effektiv kommunikation med nyckelleverantörer i säkerhetsarbetet.

På längre sikt är vaksamhet centralt för att följa föränderliga tillvägagångssätt. Att hela tiden se över sina skyddsåtgärder med stöd i regelbundna riskbedömningar och lärdomar från avslutade incidenter, säkerställer att skyddet mot överbelastningsangrepp ligger i linje med hotlandskapet.

Rapporten är ett resultat av samarbete mellan NCSC-SE, drabbade sektorer och näringslivet. Den visar att det privata och offentliga verksamheter kan samverka effektivt i att analysera cyberhot genom att dela information och resurser samt att bygga på varandras respektive styrkor. Sådant samarbete är avgörande för att göra samhället motståndskraftigt mot olika former av cyberhot på lång sikt, inte minst sådana överbelastningsangrepp som beskrivs i rapporten.

För mer information och kontakt
www.ncsc.se och ncsc@ncsc.se

Nationellt cybersäkerhetscenter NCSC

NATIONELLT
CYBERSÄKERHETSCENTER