Carl-Oskar Bohlin: Pressträff om cybersäkerhet 2026

Talare
Carl-Oskar Bohlin
Minister för civilt försvar

Datum
10 november 2026

Plats
Regeringskansliet, Stockholm

Omständigheter
Minister för civilt försvar, Carl-Oskar Bohlin och John Billow från NCSC håller pressträff angående cyberattacker mot Sverige och andra Europeiska länder. Under sensommaren och hösten 2026 attackerades matleverantörer och butiker av omfattande cyberattacker som bland annat försatte frysar att värmas upp över natten. Bohlin och Billow uppmanar allmänheten, privata aktörer och statliga aktörer att ta cybersäkerhet på allvar.

Hej och välkomna till denna pressbrief om läget på cyberområdet. Med mig har jag också John Billow, chef för det nationella cybersäkerhetscentret.

I april i år så höll vi en pressträff om risken för de potentiellt mycket allvarliga konsekvenserna vid angrepp mot de styrsystem som driver kraftvärmeverk, vattenverk och industri, som vi hade sett exempel på, men då lyckats avvärja. Idag så bygger vi vidare på detta och vill ge en lägesbild över de senaste tidens ganska uppmärksammade händelser på cyberområdet, inte minst då förra veckans angrepp mot kylsystem i svenska butiker. Så vi vill därför ge en samlad bild av läget och avsluta med några tydliga uppmaningar om vad var och en och aktörer bör göra då.

Om vi börjar med att titta på hur läget ser ut så kan vi konstatera att hotbilden skärps. FRA, MUST och Säkerhetspolisen har konstaterat att Ryssland är mer riskbenäget än tidigare och att säkerhetsläget och hotbilden mot Sverige fortsätter att försämras. Vi har sett försök till förstörande cyberangrepp, det vill säga det vi pratade om i april från Ryssland, med koppling till rysk underrättelse- och säkerhetstjänst mot svenska mål. Säkerhetspolisen ser också att Ryssland, Kina och Iran i allt högre grad samverkar med varandra och förstärker varandra. Det handlar inte längre bara om att stjäla information. De främmande makter riktar också in sig på system som styr funktioner i samhället, el, vatten och värme för att nämna några exempel. Hur kommer AI in i detta? Jo, AI gör det lättare att angripa, såtillvida att AI idag kan bidra till att hitta sårbarheter och säkerhetshål i en snabbare takt än tidigare. Antalet kända säkerhetshål i programvara har nästan fördubblats på ett års tid. Förra året så

rapporterades 48 000 kända sårbarheter och hittills i år så har det rapporterats över 86 000. Storbritanniens nationella cybersäkerhetscenter bedömer det som mycket sannolikt att AI-driven skadlig kod kommer att användas i ett utpressningsangrepp mot brittisk kritisk infrastruktur senast 2028.

Sammantaget så gör detta att den situation vi befinner oss i nu gör att tiden för att agera krymper. Säkerhetshål utnyttjats inom bara några dagar efter att de blev kända. När sårbarheten i PHP blev känd i oktober så steg försöken att utnyttja de här sårbarheterna till miljontals inom ett dygn. Myndigheter i flera av våra grannländer stängde webbplatser bland annat i förebyggande syfte. Den som inte uppdaterar sina system riskerar såtillvida att bli ett lätt byte. Sammantaget så finns det en risk att vi får se fler cyberincidenter de kommande månaderna och som chefen för Storbritanniens nationella cybersäkerhetscenter påpekade förra veckan så beror det inte på att AI har uppfunnit nya sätt att angripa oss utan på att sårbarheter som har tolererats alldeles för länge nu kan hittas i ett tempo och utnyttjas i en skala som inte tidigare har varit möjlig.

Den senaste tiden så har vi då, om man ska sammanfatta det som två uppmärksammade incidenter. Det första gäller då sårbarheten i PHP, ett programspråk som en stor del av världens webbplatser är byggda med. Och därefter så har vi då den här händelsen som kopplar till kylsystem i butiker, och där är ju inte bara Sverige som har drabbats utan vi kan konstatera att vi har haft ett angrepp på ungefär 700 butiker i Frankrike med stora materiella skador som följd av detta. I Sverige så natten mot den 2 november så drabbades ungefär 30-tal svenska matbutiker, plocklager och flera restauranger har drabbats också. Vi har också sett liknande händelser i Belgien, Estland, Finland, Irland, Luxemburg och Nederländerna. I det här skedet så går det inte att säga om det finns en koppling mellan de angrepp som ägde rum i Frankrike och de angrepp som har ägt rum i Sverige. Vi pratar här om en sårbarhet som har en relativt låg verkshöjd, det vill säga det handlar om ouppdaterade lösenord till de här kylsystemen. Det vill säga det betyder inte per se att det är samma aktör som har genomfört angreppet i Frankrike som också genomfört dem i andra länder, det här är ett angrepp som har varit lätt att kopiera för aktörer som har velat göra det, men det här är naturligtvis en fråga som nu utreds. Polisen har idag 22 ärenden kopplade till just den här incidenten. Och den gemensamma nämnaren för de här incidenterna det är alltså att angriparen har inte behövt använda någon avancerad teknik för att lyckas, utan de här systemen som stod exponerade mot internet, svaga lösenord eller kända säkerhetshål var sårbarheter

som inte hade åtgärdats och det här är en viktig detalj i sammanhanget, därför att innan den här händelsen ägde rum i Sverige, och det här kommer John säkert att berätta mer om, så har alltså det nationella cybersäkerhetscentret och CERT-SE, den del av centret som hanterar den här typen av frågor, varnat berörda aktörer för de här sårbarheterna. Ett antal av de aktörerna har då alltså inte valt att åtgärda sårbarheterna, och vi ser fortfarande att det finns aktörer i det svenska samhället som har den här typen av sårbarheter och inte har åtgärdat dem och vi kommer komma in på slutsatserna av det här i slutet, men det man kan säga redan nu sammanfattningsvis är att vi befinner oss i en miljö i cyberdomänen där vi inte har råd som samhälle att inte hantera och inte åtgärda sårbarheter snabbt nog, därför att just nu befinner vi oss i ett sammanhang där exponeringen av nya sårbarheter hela tiden accelererar till följd av AI-användningen.

Om man då ändå bara sammanfattningsvis nämner någonting innan John får ordet om vad är det vi har gjort på strukturell nivå för att försöka positionera Sverige bättre i den här miljön. Regeringskansliet presenterade ju en rapport om det nationella cybersäkerhetsarbetet mellan 2017 och 2022 på nationell nivå och gav det arbetet i stort underkänt. Vi har försökt ta fasta på detta. Vi har byggt ett nytt nationellt cybersäkerhetscenter som finns inlemmat i FRA. Vi har en ny nationell cybersäkerhetsstrategi med en årlig handlingsplan som hela tiden uppdateras för att vi ska kunna nå ett mätbart målläge 2030. Vi satsar drygt en miljard de kommande åren på förstärkt cybersäkerhet också för kommuner och regioner, därför att man hör ofta aktörer ute i myndighetssverige säga att vi behöver mer finansiering för detta. Detta har regeringen tillfört både tidigare under innevarande budget och i planen för de kommande två åren. Vi har en ny cybersäkerhetslag som ställer högre krav på alla aktörer som ägnar sig åt samhällsviktig verksamhet och vi har också ett uppdrag till det nationella cybersäkerhetscentret, ett uppdrag till FRA, Försvarsmakten om, och det sistnämnda handlar om att utveckla en AI-stödd cybersäkerhetsförmåga, och till centret är uppdraget att samordna arbetet om avancerade AI-modeller i syfte att hjälpa oss att förbättra vår cybersäkerhet.

Jag tänker att jag lämnar över ordet till John för en fördjupad lägesbild och några ord om hur ni arbetar på NCSC med detta.

Och eftersom repetition är kunskapens moder så tänkte jag avsluta med att säga att tiden för att agera, den är här och nu och den är här och nu därför att

säkerhetsläget fortsätter att försämras. Vi ser att angriparnas verktyg blir effektivare, vi ser att tiden att agera krymper och det ställer högre krav på alla som levererar samhällsviktig verksamhet. Den stora energiproducenten, det kommunala vattenbolaget och den lilla matbutiken, de har alla olika uppgifter men alla måste kunna fullgöra de här uppgifterna även under sämre och svårare förhållanden än vi möter idag och då duger det helt enkelt inte att vi har en situation där det nationella centret varnar för sårbarheter, men aktörer underlåter att agera. Det är att kompromissa med allas vår gemensamma säkerhet.

Så låt mig därför återigen understryka att cybersäkerhet är inte fritt valt arbete. Det här ansvaret måste omsättas i praktisk handling från alla aktörer som bedriver samhällsviktig verksamhet, och de rekommendationer och de varningar för sårbarheter som kommer från centret måste hörsammas och åtgärdas omedelbart, därför att tidsfönstret för att åtgärda dem krymper hela tiden.

Tack. Vi tar därmed emot frågor.

Källa
Transkriberat från videoinspelning: Pressträff om Cyberattacker, publicerad på YouTube, uppladdad av "Regeringskansliet", 10/11 2026 (Transkriberat 11/11 2026)

Taggar
Moderaterna, Politiska tal

Relaterade
John Billow: Pressträff om cybersäkerhet 2026
10 november 2026

URI
https://www.svenskatal.se/tale/carl-oskar-bohlin-presstraff-om-cybersakerhet-2026