John Billow: Pressträff om cybersäkerhet 2026

Talare
John Billow
Chef för Nationellt Cybersäkerhetscenter

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.

Tack så mycket, statsrådet.

Som sagt, den senaste tiden har vi fått ständiga påminnelser om det cyberhot som Sverige ställs inför, och förra veckans angrepp mot kylar och frysar i de här livsmedelsbutikerna och andra verksamheter, då såg vi ju sådana grundläggande sårbarheter som finns i vårt uppkopplade digitala samhälle kan utnyttjas. Jag stod här tillsammans med statsrådet för bara ett halvår sedan för att just uppmärksamma de utmaningar som finns med uppkopplade enheter som styr och övervakar fysiska processer och maskiner i industri och annan infrastruktur, det som vi brukar kalla cyberfysiska system och operativ teknik. Utmaningen består i att sådana system många gånger är äldre och designade med mindre fokus på cybersäkerhet. Det är när sådana system kopplas upp mot internet, ofta av tillgänglighets- och smidighetsskäl, som det blir möjligt att också angripa dem. Och sådana angrepp som vi har sett kan leda till samhällskonsekvenser, och särskilt då om de används i hantering av tjänster som vårt samhälle är beroende av. Angreppen förra veckan riktade sig då in sig på styrsystem för kylar och frysar, och på Nationellt cybersäkerhetscenter har vi kunnat konstatera att merparten av det drabbade systemen var från samma tillverkare, många gånger äldre system som var internetanslutna med otillräckligt skydd. Och på så sätt kunde angriparen ta kontroll över systemen och ändra deras temperaturinställningar, vilket resulterade i den skada som uppstod. Det har ännu inte kunnat gå att fastställa vem eller vilka aktörer som legat bakom de här angreppen i Sverige. Sådan analys pågår, men den är tidskrävande och det är inte alltid möjligt att i slutändan få en fullständig bild. Det kan dock konstateras att de här angreppen inte har använts för utpressning, vilket annars är vanligt i

sådana här sammanhang. I detta fall var skadan utförd redan i och med angreppet. Och jag fortsätter att mana alla till en försiktighet att dra förhastade slutsatser eller spekulera kring vilka aktörer som ligger bakom de angrepp som vi utsatts för här just nu i Sverige.

Det viktiga för oss är just nu att fokusera på det cybersäkerhetsåtgärder som behöver vidtas för att höja skyddet. Nationellt cybersäkerhetscenter har bedrivit ett omfattande kartläggningsarbete för att identifiera sårbara uppkopplade enheter i Sverige. Det uppmärksammades också tidigare under hösten. Vi har kunnat identifiera flera tusen enheter som är exponerade mot internet inom dagligvaruhandel, fastighetssystem, transport och logistik, vattenrening, energi och industriverksamheter. Och Sverige sticker ut. Vi har ett större antal exponerade och sårbart uppkopplade enheter än till exempel våra nordiska grannländer. Nationellt cybersäkerhetscenter har skickat riktade säkerhetsmeddelanden till verksamhetsutövare som vi har kunnat identifiera med sårbara uppkopplade enheter för att uppmärksamma dem på att det behöver stärka sitt skydd och vi skickade även ett 20-tal riktade meddelanden till flera verksamheter inom dagligvaruhandeln i Sverige efter kyl- och frysangreppen i Frankrike några veckor sedan, precis som Carl-Oskar nämnde här. Och flera av dem vi har varit i kontakt med har också hörsammat uppmaningen att uppgradera sitt skydd, men inte alla. I det aktuella ärendet har vi tillsammans med våra samverkansmyndigheter och partners, främst genom vår nationella funktion för hantering av it-incidenter, CERT-SE, haft ett löpande utbyte med det drabbade och erbjudit stöd och att bättre förstå hur angreppen har genomförts. Vi har även haft kontinuerlig kontakt med våra europeiska partner i andra drabbade länder och jag har personligen också haft kontakt med flera av mina motsvarigheter i Europa. I vår roll som Sveriges nationella cyberkrishanteringsmyndighet deltar vi också i lägeskonferenser med EU:s cyberkrisnätverk när denna typ av allvarliga incidenter inträffar i flera länder. Nätverkets gemensamma bedömning i detta fall, och som vi sammanfattat nyligen i ett gemensamt uttalande, var att det inte fanns behov av att eskalera incidentnivån då länderna bedömt att de hade förmåga att just hantera angreppen. Del av vår nationella samordning har skett inom ramen för Nationellt cybersäkerhetscenters arbetsgrupp för incidentkoordinering och i den ingår bland annat Polismyndigheten, Säkerhetspolisen, Myndigheten för civilt försvar och Post- och telestyrelsen. Löpande informationsutbyten har även skett med Myndigheten för civilt försvar inom deras nationella samordnande uppdrag rörande kriser och Polismyndigheten som vi hörde

ansvar för brottsutredningen av de här inträffade angreppen.

Nu är det hög tid att prioritera cybersäkerhetsarbetet. Organisationer och underleverantörer som har sån här OT-system och särskilt det som finns inom kritisk infrastruktur behöver agera och få överblick på sina utsatta system och enheter. För de cirka nu 3 500 samhällsviktiga verksamheter som cybersäkerhetslagen omfattar finns det därför nu skarpa och detaljerade krav. Vi uppmanar verksamheter att tydligt inventera uppkopplade enheter och därefter begränsa exponeringen genom säkerhetsåtgärder. Skydda era system genom att använda tekniska skyddsåtgärder, säkerställ en incidenthanteringsförmåga och ha en kontinuitetsplan för att begränsa skada vid angrepp. Det är inte enbart verksamhetsutövare som behöver agera. Länge har den stora bördan för bristfällig kvalitet i cybersäkerhet hos digitala produkter och hårdvara enbart lagts på slutanvändaren och konsumenten, nu stärks dock kraven markant på producenterna och distributörerna när EU:s cybersäkerhetsförordning börjar träda i kraft. Redan nu gäller skärpta krav på att producenter ska rapportera upptäckta sårbarheter och det görs via EU:s cybersäkerhetsmyndighet ENISA och rapporteras vidare till oss på Nationellt cybersäkerhetscenter för de svenska verksamheterna och nästa år så kommer alla uppkopplade produkter, hårdvara och mjukvara behöva designas med cybersäkerhet inbyggt och inte innehålla kända sårbarheter och de kommer gälla som krav under hela produktens livslängd. Det är ett viktigt skifte och lägger en större del av ansvaret också på de som tillhandahåller dessa uppkopplade produkter.

Vi på Nationellt cybersäkerhetscenter hanterar också även andra typer av stödjande tjänster och verksamheter kan idag anmäla sig till dessa tjänster och vi uppmanar er att göra det och ta del av våra råd och rekommendationer på vår hemsida, ncsc.se. Privatpersoner har också en roll i samhällets cybersäkerhet. Den stora ökningen av konsumentprodukter som är uppkopplade gör det viktigt att ha koll på vad man har uppkopplat i sitt hem. Hotaktörer som vill komma åt information om dig kan angripa dina enheter och utnyttja brister i dessa för att ta kontroll över dem utan att du som ägare är medveten om det. Säkerställ därför att alla dina enheter löpande hålls uppdaterade och fundera över om allt verkligen behöver vara uppkopplat. Det finns mer information och åtgärder för ett säkrare digitalt privatliv på vår hemsida. Cybersäkerhetsarbetet vi bedriver i Sverige är inte ett självändamål, det är en förutsättning för det byggda digitala fundament som behövs för vår välfärd och för vår konkurrenskraft och stark cybersäkerhet bidrar till en starkare ekonomi och ett

robust och motståndskraftigt samhälle och i det arbetet har vi alla ett ansvar att agera och bidra.

Tack så mycket.

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

Taggar
Politiska tal

Relaterade
Carl-Oskar Bohlin: Pressträff om cybersäkerhet 2026
10 november 2026

URI
https://www.svenskatal.se/tale/john-billow-presstraff-om-cybersakerhet-2026