Anna-Karin Hatt: Vi har inte råd med några svaga länkar

Talare
Anna-Karin Hatt
It- och energiminister

Datum
21 augusti 2012

Plats
Folkets Hus, Stockholm

Omständigheter
Tal på informationssäkerhetskonferens med Myndigheten för samhälle och beredskap.

Acrobat Reader: 30 000 dollarWindows: 120 000 dollarInternet Explorer: 200 000 dollarApples operativsystem: 250 000 dollar

Det här är ett axplock av priser som tidskriften Forbes publicerade tidigare i år över vad man får betala om man av någon anledning vill ha exklusiv tillgång till så kallade zero day-sårbarheter för olika program eller operativ-system, i praktiken alltså en prislapp för hur man tar sig in i en organisations it-system. Om attacken lyckas får angriparen en väg förbi alla skydd och brandväggar och därmed fullständig kontroll över ett it-system.

Nästan alla it-system har sårbarheter, men ser man bara till att ha uppdaterade system är det oftast ingen större fara eftersom man då successivt ser till att laga hålen.

Det som gör en zero day-sårbarhet dyrbar, är att den är ny och helt okänd, och därmed sannolikt inte kommer upptäckas av antivirusprogram eller brandväggar.

Sårbarheter som dessa är numera en handelsvara och det är inte bara ljusskygga hackers som ägnar sig åt detta. Tvärtom. Även här i väst finns det numera helt legitima bolag som är verksamma i den branschen. Och köparna är allt från den organiserade brottsligheten till nationella underrättelse-tjänster, i alla fall om man får tro Forbes magasin.

För två år sedan härjade masken Stuxnet, en skadlig kod som inte bara kan slå ut it-system, utan som också kan påverka fysisk utrustning och kritisk infrastruktur som kärnkraftsproduktion, vattenförsörjning, elförsörjning och

trafikledningssystem. Upphovsmännen bakom Stuxnet använde inte en, två, eller tre utan hela fyra helt separata zero day-sårbarheter för att lyckas med sina syften.

Den senaste i raden av kvalificerad skadlig kod är Flame. Flame är enligt forskarna den mest avancerade skadliga kod som någonsin upptäckts. Jag vill inte spekulera om vilka syften de som skapat Flame har eller vad konsekvenserna av den kan bli. Men en sak är säker: Vi lever i en ny värld där gamla sanningar och självklarheter inte längre gäller.

Det som idag är en säkerhetsrisk fanns för 5 år sedan knappt på agendan. Men idag kan det vara den säkerhetsrisk som vi kanske fruktar allra mest, och något som kan slå ut stora delar av vårt samhällssystem.

Digitaliseringen är fantastisk. Den ger oss både utveckling och tillväxt. Fler företag. Nya tjänster. Fler jobb. Det ökade informationsutbytet stärker vår demokrati och ger oss som medborgare och företagare nya tjänster. Ny infrastruktur byggs där alla kan ta del av informationen på nätet – oavsett kön, etnisk tillhörighet, funktionsnedsättning eller ålder. Som medborgare förväntar vi oss nu allt mer att all information och alla tjänster ska finnas tillgängliga, bara ett knapptryck bort. Allt detta är fantastiskt bra.

Men digitaliseringen gör oss också mer sårbara. Och när tekniken inte fungerar, då får vi direkt problem. Vårt moderna samhälle står allt oftare stilla när våra it-system inte fungerar.

Ta bara Trafikverkets it-haveri i somras, det som bland annat innebar att trafikledningscentralen i Göteborg inte längre kunde se på sina skärmar var tågen befann sig. Det är allvarligt i sig. Men ännu mer allvarligt blev det när inte heller plan B, backup-systemet, fungerade. Resultatet blev att man tvingades stoppa alla tåg i Västsverige och att tusentals resenärer blev försenade. Samtidigt som det tack och lov stannade vid det.

När it-system havererar kan det bero på tekniska fel, på misstag som beror på den mänskliga faktorn eller på medvetna handlingar. Men den kan också bero på externa faktorer, som extremt väder.

Ta stormarna Per, Gudrun och nu senast, efter julhelgen i fjol – stormen

Dagmar. I alla dessa blev spridningseffekterna stora och det tog lång tid att återställa alla skador. Robustheten i systemen för både tele- och elförsörjningen drabbades och sattes på verkliga prov.

Oavsett vad som ligger bakom att it-system går ner så är det gemensamma att förvarningen oftast är obefintlig, att tempot är högt och att incidentens konsekvenser får stor spridning, kanske till och med över nationsgränser.

Bristande informationssäkerhet ställer högre krav på samhällets förmåga att hantera allvarliga störningar och kriser.

Därför måste de här frågorna uppmärksammas av oss alla: av privata och offentliga aktörer, av enskilda medborgare och storföretag – för att vi ska kunna ha den goda informationssäkerhet vi behöver, i alla delar av samhället. Och mer måste göras både för att förebygga och för att hantera både mindre it-incidenter i vardagen, och större, allvarliga kriser.

Vårt samhälles krisberedskap bygger på ett antal principer. Ansvarsprincipen, som är den grundläggande principen, innebär att den som ansvarar för en verksamhet under normala förhållanden också har detta ansvar under en kris. Det ingår alltså i verksamhetsansvaret att göra allt som krävs för att skapa robusta system och se till att man kan hantera incidenter. Det arbetet måste göras i samverkan mellan olika aktörer så att vi kan förebygga och hantera allvarliga händelser och kriser på ett effektivt sätt.

För att vi ska kunna ha tillräcklig överblick och för att vi ska kunna prioritera våra insatser, särskilt vid allvarligare händelser som berör flera sektorer, behöver vi ha en gemensam lägesuppfattning. Den gemensamma lägesuppfattningen måste bygga på ett samordnat informationsutbyte där det förebyggande arbetet inte glöms bort.

För snart ett år sedan presenterades den digitala agendan för Sverige, regeringens helhetsperspektiv inom it-området. I den slår regeringen fast att vi i Sverige ska vara bäst i världen på att använda digitaliseringens möjligheter. Ska vi lyckas med det måste vi som medborgare och företagare ha förtroende för våra it-system. Och det kommer bara bli viktigare i framtiden. Att kunna garantera en säker, motståndskraftig och tillförlitlig elektronisk kommunikationsmiljö är en framtidsfråga för Sverige och för alla världens länder.

Informationssamhällets säkerhet och integritet är en stor nationell utmaning. Den är av strategisk betydelse för såväl svensk utrikes- och säkerhetspolitik som för vårt näringsliv, för vår innovationskraft och för vår tillväxt.

I detta arbete har näringslivet en betydelsefull och viktig roll som den största ägaren och förvaltaren av denna viktiga infrastruktur. Och detta faktum ställer ökade krav på oss att klara samverkan. Kanske är det till och med så att vi behöver ett nytt kontrakt mellan det privata och det offentliga för hur vi kan samverka och gemensamt göra samhället säkrare.

Förmodligen är det oundvikligt att samhällsviktiga verksamheter då och då drabbas av it-incidenter.

Ingen här inne har glömt Tieto-haveriet förra året, som ledde till att recept på våra apotek inte kunde expedieras, till att kommunala e-tjänster slogs ut och till att fullt fungerande bilar fick körförbud eftersom godkända kontrollbesiktningar inte gick att rapportera in.

Allt fler av våra system integreras nu , precis som i Tieto:s fall, med varandra och samlas i en enda central miljö. Och det är många gånger rationellt, sparar kostnader och minskar vårt energibehov. Men det leder samtidigt till att ett tekniskt fel snabbt kan leda till avbrott i flera system, lite som ringar som sprider sig på vattnet. Och i slutändan kan konsekvenserna för samhället bli väldigt allvarliga.

Det ställer också stora krav på samordning och samverkan. På att varje organisation ser över vilka verktyg man har till sitt förfogande. Ett sådant viktigt verktyg är den offentliga upphandlingen och att bli bättre på att ställa krav och upphandla rätt. Och just när det gäller offentlig upphandling återstår mycket fortfarande att göra, vilket Riksrevisionen nyligen pekat på.

I den digitala agendan för Sverige pekar regeringen på hur viktigt det är att vi i det offentliga faktiskt vet hur man upphandlar lösningar för säker informationshantering. Vet vi det så kan det i förlängningen också sätta viktiga standarder för informationssäkerhet. Drar vi dessutom nytta av Kammarkollegiets kompetens när vi upphandlar kan vi ytterligare förbättra informationssäkerheten i den offentliga förvaltningen.

Ett viktigt sätt att bli bättre är att helt enkelt lära sig av de incidenter som inträffar.

Erfarenheterna från Tieto visar att vi måste bli bättre på att snabbt skaffa oss en korrekt lägesbild, på att uppfatta vilka konsekvenser som kan bli följden och på att se vad som snabbt måste göras för att minimera skadorna.

Rätt information om hur läget ser ut är en förutsättning för att alla inblandade aktörer ska få samma förståelse för situationen och kunna vidta samordnade åtgärder. Ska man kunna få en sådan viktigt lägesbild i kris förutsätter det att man har kontinuerlig kontakt med nyckelaktörer inom och utanför landet, också när det inte är kris.

En annan förutsättning för att vi ska ha en korrekt lägesbild är att it-incidenter verkligen rapporteras in. Och faktum är att det idag saknas en sådan systematik, vilket gör att ansvariga myndigheter får svårare att snabbt skapa sig en riktig lägesbild.

Samtidigt måste vi bli bättre på det som kallas kontinuitetsplanering, på att se till så att varje aktör på förhand tänker igenom vad som skulle hända om de it-system man använder slutar att fungera. När något väl inträffar ska man vara så väl förberedd att man har en förberedd plan B, som kan sättas igång och som fungerar.

För att vara kristallklar; dagens frivilliga rapportering av it-incidenter räcker inte för våra behov. Just därför har jag och regeringen givit MSB i uppdrag att titta på hur ett system för obligatorisk it-incidentrapportering för statliga myndigheter kan se ut.

Därför att med en bättre lägesbild skulle våra myndigheter kunna angripa komplexa problem på ett mycket mer effektivt sätt.

Och det kräver bättre samverkan mellan våra myndigheter och mellan våra myndigheter och näringslivet. Uppdragets huvudfokus är de statliga myndigheterna. Men vi vet att viktiga offentliga funktioner kan bli väldigt lidande när privata företag drabbas av avbrott. Jag vill att Sverige ska få ett verkligt fungerande system för inrapportering av it-incidenter. Och skulle MSB

komma fram till att företag, under vissa omständigheter, behöver omfattas av ett sådant inrapporteringskrav för att vi ska få ett system som fungerar – ja då har de också möjlighet att föreslå det.

För att vi ska veta vad som behöver göras behöver alla berörda organisationer göra risk- och sårbarhetsanalyser. Och man behöver samtidigt fundera över riskanalyser och hur man ska klassificera information. Och vill man kan man gärna ta stöd av MSB i det arbetet.

En av flera viktiga förutsättningar för att man ska kunna förebygga och hantera it-incidenter är informationsdelning. Att man klarar av att göra relevant information tillgänglig i rätt tid, till rätt aktör, på ett säkert sätt. Information som ofta finns hos både privata och offentliga aktörer, nationella och internationella. För att den informationsdelningen ska fungera måste det finnas ett ömsesidigt förtroende mellan de berörda aktörerna, både i den privata och i den offentliga sektorn.

It-attacker genomförs på en rad olika sätt och med många olika syften. Varje dag, året om, förmodligen just nu, bedrivs det avancerade operationer mot svenska intressen. Och det är inte bara tonårspojkar som dricker jolt cola som ligger bakom dem, utan många gånger långt mer kvalificerade aktörer med betydande resurser. Det är inget vi behöver gissa oss till. Det är något vi vet.

Sverige är ett högteknologiskt land med många företag som ligger i den absoluta framkanten. Det gör oss också till ett attraktivt land att bedriva spionage mot, att rikta destruktiva angrepp mot eller att använda i förberedelser för andra angrepp. Allt detta görs ofta utan systemägarens kännedom. Därför har jag givit Försvarets radioanstalt i uppdrag att lämna förslag på hur ett tekniskt varnings- och detekteringssystem som ska kunna upptäcka denna typ av sofistikerade angrepp kan se ut.

Så sent som igår redovisade MSB en uppdaterad version av Sveriges nationella handlingsplan för informationssäkerhet, den som Krisberedskapsmyndigheten år 2007 fick i uppdrag att ta fram. Deras arbete har skett i samverkan med SAMFI-myndigheterna, dvs. Försvarets materielverk, Försvarets radioanstalt, Försvarsmakten, Polismyndigheterna och Post- och Telestyrelsen.

Den nationella handlingsplanen för informationssäkerhet vänder sig till alla

aktörer i samhället och särskilt till dem i viktiga infrastrukturområden som transporter, energiförsörjning och finanssektorn. Handlingsplanen innehåller 27 konkreta åtgärdsförslag, allt från ökad användning av certifierade produkter och system, till uppföljning av säkerheten inom elektronisk kommunikation och till att öka säkerheten i industriella informations- och styrsystem.

Det är bra. Men eftersom informationssäkerhet är en horisontell fråga som skär genom alla sektorer behövs också ett brett samhällsperspektiv. Och därför tror jag att vi också – vid sidan av handlingsplanen – behöver en ny bred, nationell strategi för informationssäkerhet. Vi behöver en bättre helhetssyn i vårt samhälle på vad som ska skyddas, vilka hoten är och vilka medel vi ska ha för att förstärka vårt skydd.

Det handlar om allt från säkerhets- och försvarspolitiska aspekter, medborgerliga rättigheter, integritetsfrågor, brottsbekämpning till säkerhet i vardagen. Jag vill att en sådan ny nationell strategi för informationssäkerhet ska möjliggöra en samlad politik och omfatta arbete med informationssäkerhet på alla nivåer och områden i samhället. Jag ser framför mig att en sådan ny nationell strategi ska bli ett övergripande sammanhållet ramverk för hur arbetet med informationssäkerhet ska bedrivas i Sverige.

Och när vi väl har en sådan strategi på plats, så kan vi skapa mer detaljerade riktlinjer och handlingsplaner för olika områden och sektorer. Den uppdaterade handlingsplanen från MSB som kom igår, kommer vara ett av flera underlag till den nya informationssäkerhetsstrategin. Nu vidtar ett brett arbete med att utforma en ny bred strategi. Jag välkomnar alla era inspel i det arbetet.

Förhoppningsvis kan vi gemensamt se till så att den där prislistan över sårbarheter som jag nämnde i början i framtiden blir irrelevant, därför att vi har brandväggar, för att vi har redundans och inte minst för att vi har medvetna användare som gör att våra system är skyddade.

För att sluta där jag började: Det haveri som drabbade tågtrafiken i Västsverige nu i somras. Det när tågen stod stilla i nästan 4 timmar. Jag vet nu vad det berodde på. I Göteborg finns det nämligen en driftledningscentral som övervakar all trafik på den västra stambanan. Och man hade gjort en hel del av sin hemläxa och säkrat all kommunikation till den centralen, enligt konstens alla regler, med redundans, driftsäkerhet, ja precis allt som behövs. Och

kommunikationen från centralen var precis lika säker.

Men hur såg det ut inne i det egna huset, där centralen satt? Jo, all kritisk data passerade en helt vanlig nätverksswitch som inte ens var övervakad. Och just den switchen började krångla vilket gjorde att ledningscentralen inte kunde se tågens positioner och all trafik fick stoppas av säkerhetsskäl. På grund av att switchen inte var övervakad tog det timmar innan man ens kunde se var felet satt.

Ingen kedja är starkare än sin svagaste länk. Alla de miljontals kronor som hade lagts ned i driftssäkerhet räckte inte, när en vanlig obevakad switch började krångla.

Jag räknar med att alla ni här inne funderar lite över hur det ser ut i er organisation. Var någonstans står er obevakade switch? Vilken är er svagaste länk?

Det är min övertygelse att vi bäst hittar svaga länkar genom att tänka brett och systematiskt, och genom att bli bättre på att samverka över sektorsgränser och mellan myndigheter. Med den nya nationella strategin för informationssäkerhet tar vi nästa steg för ett samhälle där vi kan lita på att information inte läcker, där tågen kan gå i tid och där brandväggar håller våra system säkra.

Taggar
2010-tal, 2012, Centerpartiet, Kvinna

URI
https://www.svenskatal.se/tale/anna-karin-hatt-vi-har-inte-rad-med-nagra-svaga-lankar