SVENSKT NÄRINGSLIV

FÖRETAGEN OCH IT-SÄKERHETEN – hotbilder, motåtgärder och behov

RESULTATEN AV EN INTERVJUUNDERSÖKNING MED SÄKERHETSANSVARIGA I ETT REPRESENTATIVT URVAL AV FÖRETAGEN I STOCKHOLMSBÖRSENS SÅ KALLADE OMX30-INDEX

MARS 2021

Innehåll

Sammanfattning

- Industrispionage och cyberangrepp kan på goda grunder anses orsaka näringslivet mycket stora kostnader, och stora andra ekonomiska förluster, varje år.
- Många företag är en del av den samhällskritiska infrastrukturen.
- De flesta företag (och också andra organisationer) saknar ekonomiska och personella resurser för att på ett adekvat sätt möta de säkerhetsutmaningar som följer med det digitaliserade samhället.
- Hotet om industrispionage och förekomsten av cyberangrepp är vardag för alla stora företag. Cyberangreppen bedrivs i närmast industriell skala, och kan närmast jämföras med en aldrig avtagande flodvåg som nöter på företagens it-infrastruktur.
- Om Sverige ska kunna möta de tekniska och ekonomiska utmaningar som ett digitaliserat samhälle innebär så måste den svenska staten och dess myndigheter börja inse dessa utmaningars vidd, och vidta lämpliga och effektiva åtgärder.
- Det som nu krävs är att staten snarast:
  - Ger det nationella centrumet för cybersäkerhet större resurser och klart mandat att arbeta operativt – också för skydd av svenska företag. På lite längre sikt måste någon form av funktion inrättas, med det uttryckliga syftet och tillräckliga resurserna för att i praktisk handling stötta hela det svenska civilsamhället i kampen mot cyberbrottsligheten.
  - Göra det möjligt att sekretesskyddat inhämta information från näringslivet om pågående och nya hot, samt att delge näringslivet adekvat och korrekt information även om detta innebär en ändring av de svenska sekretessbestämmelserna.
  - Stärka polisens resurser för att kunna ingripa mot cyberbrottslighet.
  - Öka antalet utbildningsplatser för it-säkerhet.

Förord

Ingen kan ha undgått att notera hur digitaliseringen griper in i våra liv. Snart sagt varje funktion i vårt samhälle är beroende av en kontinuerlig elförsörjning, och av att de digitala stödsystemen fungerar. Företagen har varit ledande i utvecklingen av att nyttiggöra digitaliseringens effektivitetspotential. De har också fått erfara riskerna med denna utveckling.

För närvarande bedrivs ett brett arbete från statens sida med att bygga upp såväl ett relevant militärt försvar som ett civilt försvar. Det sistnämndas funktionsduglighet kommer att vara helt avgörande för Sveriges förmåga att värja sig i ett läge med höjd beredskap, eller i värsta fall krig.

Företagen utgör den viktigaste komponenten i det maskineri som skapar de resurser som behövs för att bygga upp ett försvar, såväl civilt som militärt. Det vore därför önskvärt att de i högre grad än nu omfattades av det skydd och det stöd som myndigheter redan erhåller.

Som denna undersökning visar är företagen redan i fredstid utsatta för ständiga attacker – både från kriminella element, och vad som i flera fall på goda grunder kan antas vara främmande makt. Företagen försöker skydda sig så gott det går, men i händelse av en konflikt som berör Sverige som stat kan de komma till korta.

Det är sannolikt att industrispionage och cyberangrepp förorsakar svenska företag kostnader i mångmiljardklassen varje år. Om våra politiker menar allvar med talet om att bygga upp ett nytt totalförsvar så måste också de företag som skapar de nödvändiga resurserna ges ett bättre skydd och mer stöd – inte i en avlägsen framtid, utan här och nu.

Thomas Lundin
Ordförande
Näringslivets Säkerhetsdelegation

Om undersökningen

Svenskt Näringsliv har utgått från hypotesen att det är de största och mest ekonomiskt betydelsefulla svenska företagen som

1. utsätts för flest illegala angrepp, både generellt och speciellt
2. har störst ekonomiskt incitament att skydda sig mot diverse angrepp
3. har de största resurserna att sätta in skyddsåtgärder
4. besitter eller köper in den bästa kompetensen på skyddsområdet.

Mot den bakgrunden har Svenskt Näringsliv under hösten 2020 genomfört en intervjuundersökning med säkerhetsansvariga i ett representativt urval av företagen i Stockholmsbörsens så kallade OMX30-index. Syftet har varit att skapa ett underlag som kan belysa företagens problem på områdena industrispionage[1] och it-säkerhet.

När det gäller de ekonomiska skadeverkningarna av problemen är osäkerheten om deras omfattning och vidd i vetenskaplig mening okänd. Benägenheten att anmäla angrepp till rättsvårdande myndigheter är svag och det gäller generellt i den större delen av världen. Detsamma gäller när det handlar om att redovisa vilka förluster som företag har åsamkats på grund av industrispionage och cyberangrepp. Detta beror på ett flertal faktorer, framför allt sådana som skulle kunna tänkas drabba företagets anseende – och därmed kunna skada både dess rykte som en seriös och pålitlig partner och dess börsvärde. Trots svårigheterna med att erhålla tillförlitliga uppgifter, har det internationellt gjorts vissa försök att beräkna skadeverkningarna. Den amerikanska *Intellectual Property Commission* uppskattade 2017 att förlusterna i USA:s näringsliv på grund av spionage, cyberangrepp och stöld av intellektuell egendom årligen uppgick till mellan 1 och 3 procent av landets BNP. I valutatermer talar vi då om 200 till 600 miljarder dollar per år. Det tyska industriförbundet BDI uppskattade 2019 att det tyska näringslivet under åren 2017–2018 orsakades skador på grund av samma typ av angrepp till ett värde av 205 miljarder euro. Det motsvarar i svenska kronor drygt 2 biljoner. Någon total uppskattning av motsvarande slag för svensk del finns för närvarande inte såvitt Svenskt Näringsliv känner till.

Fler än 14 företag har deltagit i intervjuerna och de medverkande företagen omsatte 2019 betydligt mer än 1 200 miljarder kronor och hade fler än 500 000 anställda i hela världen, varav fler än 70 000 i Sverige. Vissa har medverkat endast under förut-

[1] I den engelsktalande delen av världen brukar man skilja mellan så kallad *economic espionage* och *industrial espionage*. Med det förstnämnda avses sådan illegal inhämtning som bedrivs av stater i syfte att förstärka det egna näringslivets konkurrenskraft generellt. Med det sistnämnda avses sådan illegal inhämtning som bedrivs av oseriösa konkurrenter på marknaden. För enkelhetens skull har vi i denna rapport valt att endast använda det sistnämnda uttrycket.

sättning att deras svar inte redovisas, inte ens i schabloniserad form. Samtliga företags medverkan har byggt på ett löfte om strikt konfidentialitet och därför namnges inget företag, vare sig i fråga om de medverkat eller ej, eller beträffande vilka branscher de representerar.

De svar som redovisas i slutet av denna rapport är schabloniserade för att säkerställa anonymitet. Alla frågor har inte varit lika väsentliga för alla företag och med hänsyn till allmän läsbarhet har svaren på frågorna justerats språkligt.

Hotbilder

Fler än hälften av de intervjuade företagen anser sig ha blivit utsatta för industrispionage eller försök till industrispionage. Det har inte handlat om normal konkurrentbevakning eller så kallad reverse engineering med mera, utan illegala angrepp av olika slag som syftar till att komma åt företagshemligheter. Mindre än hälften av företagen vågar inte ha någon uppfattning om blivit utsatta för industrispionage eller försök till industrispionage. Att så många som fler än hälften svarat jakande på frågan tar Svenskt Näringsliv därför till intäkt för att industrispionage mot stora företag är vanligt förekommande.

Beträffande de metoder som använts är de företag som blivit utsatta mycket tystlåtna. Man kan dock av materialet förstå att informationsinhämtningen kan ha skett genom så kallade insiders – egna anställda, via kunder eller underleverantörer, eller genom dataintrång. Direkt fysiska angrepp i form av inbrott och stöld bedöms vara sällsynta även om stöld eller otillåten användning av persondatorer – särskilt vid distansarbete – ger en angripare större möjligheter till åtkomst. Materialet ger alltså inte tillräckligt underlag för att avgöra vilken metod som är mest vanlig, eller mest effektiv. Angrepp mot företagens it-system är emellertid så extremt vanliga och ihållande att ett sådant förfarande rimligen borde erbjuda en angripare den mest kostnadseffektiva vägen att erhålla den önskade informationen.

På frågan om industrispionaget lett till ekonomiska förluster är företagen ännu mer tystlåtna. Inga belopp har angetts och man har varit ovillig att hänföra ett visst angrepp till en specifik ekonomisk skada.

När det gäller den mer vanliga cyberbrottsligheten är företagen samstämmiga. De beskriver samtliga en miljö där angrepp av olika slag mot företagens it-system är mycket omfattande. Det kan beskrivas som en ständigt rullande flodvåg av cyberangrepp som negativt påverkar företagens digitala infrastruktur – den infrastruktur som är helt avgörande för företagens verksamhet och konkurrenskraft med mera. Det är uppenbart att utvecklingen av digital teknik har gjort det både lättare, billigare och mer riskfritt att genomföra illegala angrepp, främst syftande till ekonomisk vinning. Kriminella aktörer anges av nästan alla företagen som den vanligaste kategorin av angripare, även om statliga aktörer och så kallade hackare eller diverse aktivister i undantagsfall också kan utgöra ett störningsmoment. Det finns ett osäkerhetsmoment kring denna uppfattning eftersom de mest avancerade kriminella aktörerna bedöms ligga i nivå med statliga aktörer avseende teknisk skicklighet. Företagen bedömer också att statliga uppdragsgivare ibland använder sig av kriminella aktörer, i syfte att skapa en täckmantel. Ett särskilt problem är att företagen, utan att kunna antagas ha varit förstahandsmålet, kan bli offer för skadlig programvara som spritts med annan mottagare eller ett visst allmänt förekommande system i sikte. Cyberbrottsligheten

bedöms ha nått en omfattning som närmast kan beskrivas som industriell. Graden av sofistikering är mycket hög. Det är inte enstaka datanördar i mammas källare, utan mycket väl utbildade ingenjörer och programmerare som i organiserade former bedriver informationsstölder – för vidareförsäljning – och utpressning.

En fråga som rönt viss uppmärksamhet under senare tid har varit säkerhetsnivåerna i det som kallas för molntjänster. Dessa tillhandahålls vanligen av mycket stora företag baserade i USA. Inom EU har säkerheten, särskilt för uppgifter hänförliga till fysiska personer, ifrågasatts. Detta verkar inte vara ett problem för företagen. De anser generellt sett att det inte finns något ekonomiskt försvarbart alternativ till att använda dessa tjänster, att säkerhetsnivåerna är fullt tillräckliga för företagens behov (om man har förmåga att utnyttja dem), och att den lilla mängd företagsinformation som måste behållas i egna system kan hanteras med särskilda åtgärder. Det kan finnas tillfällen då extra försiktighet kan vara motiverad, men generellt sett inte.

Motåtgärder

Hotmiljön har gjort det helt nödvändigt för företagen att investera i säkerhetspersonal och säkerhetssystem. Enbart hotet av en inskränkning i någon del av produktionen räcker för att motivera de avsevärda kostnader som säkerhetsåtgärderna medför. Till detta kommer att vissa företag är underkastade statlig reglering i olika former som gör det obligatoriskt att upprätthålla en viss standard avseende it-säkerheten. Nivån på säkerhetssystemen varierar därför mellan företagen och om nivån är tillräckligt hög eller inte beror i slutänden vad som kan anses vara företagsekonomiskt försvarbart. Även om företagens uppgifter om direkta förluster på grund av cyberangrepp inte är klarlagda eller redovisas fullt ut så drar ändå Svenskt Näringsliv slutsatsen att produktionsbortfall, och säkert också annan skada för kunder och leverantörer samt goodwill-förlust, väger tungt i företagens kalkyl.

Kostnaderna för säkerhetsåtgärder är under alla omständigheter mycket betydande, och vi bedömer att de kommer att öka, också proportionellt, allt eftersom. Som nämnts upprätthåller olika företag olika hög standard, allt efter vad som bedöms motiverat. Vissa företag håller en mycket hög säkerhetsnivå och lägger hundratals miljoner kronor per år på dylika åtgärder. Andra företag vill inte uppge några belopp med hänvisning till definitionssvårigheter och en del vill inte lämna någon uppgift över huvud taget. Vår bedömning – grundad bland annat på underhandsuppgifter – är att enbart företagen på OMX30-listan varje år spenderar mångmiljardbelopp på säkerhetsåtgärder, i all synnerhet avseende sina it-system.

Rättsliga åtgärder eller polisanmälan vid misstänkta brott bedöms av nästan samtliga företag inte vara ett alternativ som de väljer.

Företagens behov

Som redovisas ovan anser företagen att rättsväsendet är helt otillräckligt, såväl avseende resurser som kompetens, för att kunna hantera cyberbrottsligheten. Man anser också att den svenska statsmakten generellt sett inte inser problemets vidd, och inte heller visar några tecken på att vidta lämpliga skyddsåtgärder för annat än statens eget behov. Flera företag har framhållit att andra europeiska länder vidtar åtgärder för att skydda sitt eget näringsliv – även om det lokalt verksamma företaget råkar vara svenskt. Som positiva exempel nämns särskilt Storbritannien, Nederländerna, Tyskland och Finland. Var beträffar USA har det flera gånger framhållits att den federala polisen, FBI, utgör ett föredöme när det gäller hjälp och stöd vid kriminella it-angrepp. EU:s it-säkerhetsmyndighet Enisa är så gott som okänd för företagen eller anses generellt sett inte kunna fylla rollen av konkret stödgivare.

Vissa företag upprätthåller informella kontakter med säkerhetsmyndigheterna, men dessa bedöms vara osäkra, inte formellt sanktionerade och dessutom omfattas de av sekretessregler som försvårar för företagen att få relevant information.

Allmänt sett signalerar företagens svar stark frustration eller uppgivenhet avseende den svenska statens vilja och förmåga att skydda landets näringsliv. Företagen har helt enkelt svårt att förstå varför politiken bortser från behoven hos de företag som i stor utsträckning skapar de resurser som bygger samhället. Det nationella centrum för cybersäkerhet som nu ska byggas upp kommer sent och får alldeles för små resurser. Därtill finns det starka tvivel på att den förvaltningsmodell som valts kommer att bli särskilt effektiv.

Ett särskilt problem som företagen lyfter fram är tillgången till relevant utbildad arbetskraft på it-säkerhetsområdet. Efterfrågan är mycket stor och för närvarande är säkerhetsutbildad personal en mycket trång sektor.

Små och medelstora företag

Det har inom ramen för denna undersökning inte funnits utrymme för att intervjua ett representativt urval av små och medelstora företag. Svenskt Näringsliv har istället valt att tala med med tre erfarna säkerhetskonsulter, vilka i sina respektive verksamheter också kunnat berätta om den verklighet som möter mindre företag. Dessa samtal redovisas längst bak i denna rapport.

Resultatet av samtalen är att små och medelstora företag, med undantag för industrispionage, generellt sett utsätts i samma omfattning av it-angrepp som de stora företagen. De befinner sig emellertid i en mycket sämre position, eftersom de inte har vare sig resurser eller kompetens för att hantera säkerhetshoten på ett effektivt och lämpligt sätt. De har i likhet med de stora företagen inte heller någonstans att vända sig för generellt stöd eller rådgivning.

Föreningen Svenskt Näringslivs ståndpunkter

Svenskt Näringsliv anser att följande fyra åtgärder från statens sida är mest angelägna för närvarande:

- Det är uppenbart att det svenska civilsamhället (utanför de riktigt stora företagen) saknar de resurser som krävs för att på ett lämpligt och effektivt sätt möta de hot som det digitaliserade samhället medför. Det är nästan uteslutande bara inom statens säkerhetsorganisationer som den främsta kompetensen på området för närvarande finns i Sverige. Staten måste därför snarast finna en lösning och funktion som har till huvudsaklig och uttrycklig uppgift att praktiskt stötta det svenska civilsamhället – både företag och andra organisationer som inte är myndigheter – avseende it-säkerhet. En sådan funktion måste även ges tillräckliga resurser för att lösa sin uppgift. Den organisatoriska form som valts för det planerade nationella centrumet för it-säkerhet bedömer vi inte kommer att fungera effektivt. En bättre förebild finns för närvarande i Storbritannien.
- Det finns en tydlig bild att den svenska staten inte tar hoten mot dess civila näringsliv på fullt allvar. Det finns inga tillräckligt verkningsfulla och uthålliga strukturer för att både ta emot information om säkerhetshot och att delge näringslivet och det övriga civilsamhället information om it-relaterade säkerhetshot. Staten bör därför även inrätta en funktion dit näringslivet sekretesskyddat kan delge sina säkerhetsproblem och även kan få aktuell, korrekt och relevant information om nya säkerhetshot. Detta kan innebära att den svenska sekretesslagstiftningen kan behöva ändras.
- Den civila polisen saknar idag personella, tekniska eller ekonomiska resurser för att på ett effektivt och lämpligt sätt kunna ingripa mot cyberbrottsligheten. De flesta storföretag anser att en polisanmälan i praktiken är ett slöseri med tid. Polisens resurser och prioritering av it-säkerhetsområdet kräver en kraftig förstärkning.
- Det är uppenbart att gott utbildad och talrik arbetskraft på it-säkerhetsområdet utgör en viktig förutsättning för både näringslivets och statens möjligheter att möta det digitaliserade samhällets utmaningar. Idag är detta en trång sektor som upplevs som ett problem för företagen. Detta är en omständighet som näringslivet inte ensamt kan råda bot på och staten bör därför snarast säkerställa att fler utbildningsmöjligheter på it-säkerhetsområdet skapas.

Svenskt Näringsliv har under hösten 2020 genomfört intervjuer med säkerhetsansvariga i ett representativt urval av OMX30-företagen. 14 företags svar på ett antal standardiserade frågor redovisas här schablonmässigt. Emellertid har fler än 14 företag medverkat. Vissa vill inte att deras svar ska redovisas, ens i förenklad form.

Företagsintervjuer

Företag 1

FRÅGOR

Omfattning

1. Har ni utsatts för industrispionage (varmed avses olaglig eller obehörig inhämtning av företagshemligheter, oavsett metod)?

   Nej, inte såvitt känt.

A. Har ni utsatts för cyberbrottslighet (varmed avses obehörigt intrång i eller sabotage av dataföretagets system)? + frågorna nedan

   Ja

2. Vilket/vilka tillvägagångssätt har använts?

   Phishing-attacker har syftat till att fullborda bedrägerier av olika slag. Beträffande så kallade insiderrelaterade brott av detta slag är förövarna så vitt känt inte högkvalificerade.

3. Vilken omfattning och frekvens har denna verksamhet haft?

   Så kallade DDOS-attacker och så kallad phishing sker dagligen eller flera gånger per vecka. Rent fysiska ingrepp är mycket sällsynta. (Som en sidoanmärkning: det omfattande hemmaarbetet som en följd av corona bedöms medföra ökad risk för att medarbetare kan utsättas för rån och dylikt i hemmet – i avsikt att komma över inloggningsuppgifter.)

4. Under hur lång tid har angreppen pågått?

   Cyberangreppen pågår ständigt, särskilt phishing. Massangrepp av typ DDOS bedöms ej vara riktade mot företaget som sådant. Dessa kan pågå under en eller några dagar, men hittills vid något tillfälle under en hel vecka.

5. Vilken sorts information är det som har inhämtats och i vilken form?

   Sådan som kan användas för bedrägeri av olika slag – namn, lösenord, kontouppgifter av skilda typer. Oftast är det tekniska brister som medför att uppgifter av olika slag kan läcka ut.

6. Vilka särskilda konsekvenser bedömer ni att angreppen medfört för ert företag?

   De genererar ett ständigt behov av investeringar i personalutbildning och tekniska hjälpmedel.

7. Hur stora kostnader kan de fullbordade angreppen antas ha medfört i affärsmässigt hänseende?

   Inget ungefärligt belopp anges, men uppges vara ”ej betydande”.

8. Har ni vidtagit några skyddsåtgärder med anledning av angreppen?

   Ja

9. Om ja – vilka skyddsåtgärder?

   Det viktigaste är att undvika skada genom att förebygga angrepp. Grunden utgörs av en ständig inhämtning av underrättelser som ger underlag för en utvärdering av vilka hot som förekommer, eller kan komma att sättas i verket. Man spårar kontinuerligt anomalier i sina dataflöden, förändrar vid behov sin organisation eller sina rutiner. Personal utbildas löpande och skolas till högre medvetenhet om säkerhetsrisker i verksamheten. Teknisk personal är bättre medveten om risker än den affärsmässigt verksamma. Utbildningen måste anpassas efter individernas förutsättningar för att ge effekt. Ett särskilt problem är så kallade clickmail av hög kvalitet (inte omedelbart genomskådliga, med gott språk och professionellt utformade) som riktar in sig mot individers psykologiska svagheter.

10. Hur stora kostnader kan skyddsåtgärderna antas ha medfört?

    Inget belopp anges, men kan antas vara mycket betydande. Tillgången till kvalificerad personal är en särskilt trång sektor.

11. Vilka bedömer ni är de mest frekventa aktörerna: konkurrentföretag/främmande makt/kriminella/anställda/annan aktör?

    I allt väsentligt bedöms kriminella vara den viktigaste angripargruppen. I särskilda – men sällsynta – fall bedöms främmande makt kunna ligga bakom.

12. Vilka angripare bedömer ni vara mest problematiska/svårast att motverka?

    Angrepp från främmande makt kan antas vara de mest kvalificerade, men kriminella grupperingar har nått en sådan grad av teknisk sofistikering att skillnaden mellan dem och en stat sannolikt är hårfin. Därtill kommer att stater kan använda kriminella grupperingar för att så att säga maskera sin egen inblandning och skapa förnekandepotential.

13. Har ni någon gång vidtagit rättsliga åtgärder för att motverka angrepp?

    Bedrägerier eller försök därtill polisanmäls alltid. Beträffande phishing och DDOS-attacker är denna åtgärd helt meningslös, både på grund av svårigheten att härleda brottet till enskilda gärningsmän och på grund av polisens bristfälliga resurser på området. Det kan förekomma viss samverkan med enskilda myndigheter i fall där angreppet är särskilt svårt eller långvarigt, men dessa tillfällen är mycket sällsynta.

14. Har dessa åtgärder lett till något resultat?

    Vid något tillfälle där polisen ingripit mot phishing-nätverk har man sett att angreppen avtagit temporärt.

15. Hur ser ni på den svenska statens förmåga att skydda svenska företag mot dessa angrepp och att stödja dem avseende påföljande skyddsåtgärder?

    Förmågan bedöms som låg. Det finns förvisso god kompetens inom de myndigheter som ägnar sig åt att skydda rikets säkerhet, men de gör – såvitt känt – inget för att skydda svenska ekonomiska intressen. Det förekommer – så vitt känt – inte heller något formaliserat kunskaps- och erfarenhetsutbyte med svenska företag. Polisen har inte resurser och politiken är ointresserad. Förvisso förekommer det informella kontakter med olika myndigheter, men dessa är inte officiellt sanktionerade och baseras helt och hållet på personkännedom och förtroende.

16. Hur ser ni på EU:s förmåga att skydda och stödja unionens företag i ovan avseende?

    Några enskilda medlemsstater har mycket god kompetens, och samarbetar – som det på goda grunder kan antas – med sina nationella storföretag. Unionen som sådan har inga sådana resurser.

17. Vilka statliga policyförändringar skulle ni vilja se avseende bekämpning av industrispionage/cyberbrottslighet?

    Det behövs en officiellt sanktionerad verksamhet där företag i brottsförebyggande syfte delges information som kan stödja dem i deras eget brottsförebyggande syfte. Den nuvarande svenska linjen, med vattentäta skott mellan och inom myndigheter, för att inte tala om mellan myndigheter och företag, är i längden ohållbar. Bedrägerier och phishing är något som allmänheten och politiker kan förstå, men det som stort sker sker tyst – och bedöms generera politiskt intresse först när en katastrofal skada har drabbat ett svenskt företag. Inrättandet av ett nationellt centrum för cybersäkerhet är ett bra initiativ, men om det ska medföra några positiva effekter för näringslivet så måste det också innefatta att information av brottsförebyggande karaktär delges svenska företag. Det behövs en skyldighet för en dylik myndighetsfunktion att samråda med och informera dem.

Avslutande kommentar om så kallade molntjänster

Särskilt beträffande så kallade molntjänster bedöms utvecklingen vara oundviklig och irreversibel – de stora systemleverantörerna kommer successivt att avveckla sin utveckling och sitt underhåll av stand-alone-system. Också företag som idag har sådana – fysiskt och tekniskt – avskilda system kommer i framtiden att tvingas in i molntjänster. Med tanke på att det bara finns ett fåtal betydande leverantörer i världen av sådana tjänster bedöms risken med koncentration i sig utgöra ett orosmoment. Detta hänför sig inte till molntjänstleverantörernas tekniska skyddsåtgärder – de bedöms vara i klass med eller överträffa statliga aktörers.

Företag 2

FRÅGOR

Omfattning

1. Har ni utsatts för industrispionage (varmed avses olaglig eller obehörig inhämtning av företagshemligheter, oavsett metod)?

   Nej, inte såvitt känt.

A. Har ni utsatts för cyberbrottslighet (varmed avses obehörigt intrång i eller sabotage av dataföretagets system)? + frågorna nedan

   Ja

2. Vilket/vilka tillvägagångssätt har använts?

   Phishing-attacker, syftande till att fullborda bedrägerier av olika slag. Skadlig kod (virus med mera) kommer ofta in i systemen.

3. Vilken omfattning och frekvens har denna verksamhet haft?

   Phishing sker dagligen eller flera gånger per vecka. Cirka 10 incidenter per dag kräver åtgärd.

4. Under hur lång tid har angreppen pågått?

   Phishing pågår ständigt. Massangrepp av typ DDOS har man ej varit drabbade av. Man tar emellertid för givet att man kan vara utsatta för riktade angrepp.

5. Vilken sorts information är det som har inhämtats och i vilken form?

   Man kan misstänka att immaterialrättslig egendom är intressant, men har för närvarande inga belägg för att sådan inhämtning skett.

6. Vilka särskilda konsekvenser bedömer ni att angreppen medfört för ert företag?

   Skydd av it-systemen är med nödvändighet en integrerad del av affärsverksamheten, även om åtgärderna aldrig så att säga kan räknas hem på affärsmässiga grunder. Det genererar ett ständigt behov av investeringar och löpande arbete. Hundratals personer är sysselsatta med it-säkerhet.

7. Hur stora kostnader kan de fullbordade angreppen antas ha medfört i affärsmässigt hänseende?

   Inget känt i detta avseende.

8. Har ni vidtagit några skyddsåtgärder med anledning av angreppen?

   Ja

9. Om ja – vilka skyddsåtgärder?

   Rutiner avsedda att försvåra angrepp/virus i systemen. Loggning. Ett arbete har inletts för att införa anomalispårning i tillverkningsprocesserna. ”Bug bounty” = belöningar till ”vita” hackare som upptäcker blottor i systemen. Säkerhet får man på köpet genom de stora systemleverantörerna.

10. Hur stora kostnader kan skyddsåtgärderna antas ha medfört?

    En beaktansvärd andel av företagets samlade it-budget används, för närvarande cirka 60 miljoner kronor/år.

11. Vilka bedömer ni är de mest frekventa aktörerna: konkurrentföretag/främmande makt/kriminella/anställda/annan aktör?

    Kriminella aktörer.

12. Vilka angripare bedömer ni vara mest problematiska/svårast att motverka?

    Phishing-angrepp i bedrägerisyfte. Dessa riktar sig mot enskilda individer men kan medföra sekundära skador i systemen.

13. Har ni någon gång vidtagit rättsliga åtgärder för att motverka angrepp?

    Bedrägerier eller försök därtill har polisanmälts vid ett fåtal tillfällen.

14. Har dessa åtgärder lett till något resultat?

    Nej

15. Hur ser ni på den svenska statens förmåga att skydda svenska företag mot dessa angrepp och att stödja dem avseende påföljande skyddsåtgärder?

    Den svenska staten är över huvud taget ingen spelare på detta område. Beträffande företagets verksamhet i USA har man dock fått stöd och hjälp från FBI.

16. Hur ser ni på EU:s förmåga att skydda och stödja unionens företag i ovan avseende?

    Ingen uppfattning

17. Vilka statliga policyförändringar skulle ni vilja se avseende bekämpning av industrispionage/cyberbrottslighet?

    Ett mer seriöst förhållningssätt till det svåra problem som cyberangrepp innebär i ekonomiskt avseende, innefattande ökade resurser för polisen att ingripa mot cyberbrottslingar. Detta kräver samarbete med andra stater, men om Sverige inte har egna resurser på området så är man ointressant som samarbetspartner.

Avslutande kommentar om så kallade molntjänster

Den politiskt negativa trenden inom EU mot molntjänster är inte hållbar. De stora molntjänstleverantörerna har mycket bättre cybersäkerhet än ett vanligt industriföretag någonsin kan förväntas uppnå.

Företag 3

FRÅGOR

Omfattning

1. Har ni utsatts för industrispionage (varmed avses olaglig eller obehörig inhämtning av företagshemligheter, oavsett metod)?

   Ja, definitivt.

A. Har ni utsatts för cyberbrottslighet (varmed avses obehörigt intrång i eller sabotage av dataföretagets system)? + frågorna nedan

   Ja

2. Vilket/vilka tillvägagångssätt har använts?

   Phishing-attacker. Skadlig kod (virus med mera) är ofta förekommande (escrow injection), liksom vid vissa tillfällen så kallade DDOS-attacker. Fysiska intrång i företagets lokaler och utrustning utomlands.

3. Vilken omfattning och frekvens har denna verksamhet haft?

   Phishing sker dagligen eller flera gånger per vecka.

4. Under hur lång tid har angreppen pågått?

   Phishing pågår ständigt.

5. Vilken sorts information är det som har inhämtats och i vilken form?

   I första hand avses att utnyttja företagets datakraft för sekundära ändamål, till exempel bitcoin-mining eller DDOS-attacker mot andra mål. I andra hand vill man få åtkomst till affärs-, trafik- eller transaktionsdata. På tredje plats förekommer utpressningsförsök, så kallad ransomware. Man bedömer att företagets teknik inte i sig är ett mål, utan i så fall snarare affärsmodeller.

6. Vilka särskilda konsekvenser bedömer ni att angreppen medfört för ert företag?

   Förlust av data, vilket i sin tur medför negativa konsekvenser i förhållande till kunder, tillsynsmyndigheter. Dålig pr och i vissa fall också till samarbetsföretag. Kostnader! Skydd av it-systemen är en integrerad del av affärsverksamheten, som också kan vara föranledd av krav från svensk eller utländsk tillsynsmyndighet.

7. Hur stora kostnader kan de fullbordade angreppen antas ha medfört i affärsmässigt hänseende?

   Inget direkt känt i detta avseende, men nödvändiga skyddsåtgärder av tillfällig karaktär kan påkalla hjälp från externa specialister, vilket lätt genererar kostnader i miljonklassen – allt beroende på angreppets svårhet.

8. Har ni vidtagit några skyddsåtgärder med anledning av angreppen?

   Ja

9. Om ja – vilka skyddsåtgärder?

   Rutiner avsedda att försvåra angrepp eller virus i systemen. Loggning. Vissa säkerhetsåtgärder köps från externa systemleverantörer. Hotbildsanalyser,

sandbox-experiment. Eget så kallat ”red team”. Externa experter anlitas för att testa säkerheten innan nya system av vital betydelse sätts i drift. Inköp av försäkringar i hundramiljonersklassen för händelse av skada.

10. Hur stora kostnader kan skyddsåtgärderna antas ha medfört?

    Cirka 250 miljoner kronor/år.

11. Vilka bedömer ni är de mest frekventa aktörerna: konkurrentföretag/främmande makt/kriminella/anställda/annan aktör?

    Kriminella aktörer.

12. Vilka angripare bedömer ni vara mest problematiska/svårast att motverka?

    Redan anställda individer, eller individer som på annat sätt fått åtkomst i systemen. Förmågan att skydda sig mot en så kallad insider är relativt låg, hur stringenta rutiner och anställningsprocedurer man än tillämpar.

13. Har ni någon gång vidtagit rättsliga åtgärder för att motverka angrepp?

    Alla brott som upptäcks polisanmäls.

14. Har dessa åtgärder lett till något resultat?

    Nej

15. Hur ser ni på den svenska statens förmåga att skydda svenska företag mot dessa angrepp och att stödja dem avseende påföljande skyddsåtgärder?

    Liten. Vissa informella kontakter finns. Företagets förmåga att skydda sig har främjats bättre av samverkan i vissa branschgemensamma organ.

16. Hur ser ni på EU:s förmåga att skydda och stödja unionens företag i ovan avseende?

    Ingen uppfattning, möjligen kan Enisa bidra med något slags standarder, inget mer. Enstaka medlemsländer har god kapacitet, till exempel Storbritanniens National Cyber Security Centre.

17. Vilka statliga policyförändringar skulle ni vilja se avseende bekämpning av industrispionage/cyberbrottslighet?

    Regeringen visar en total brist på handlingskraft genom att låta frågan om ett nationellt cybersäkerhetscentrum för Sverige dra ut på tiden. Den valda modellen med samverkan mellan ett antal myndigheter, där ingen har det övergripande ansvaret, kommer inte att ge några resultat. Därtill är satsningen i pengar räknat alldeles för liten.

Avslutande kommentar om så kallade molntjänster

Den politiskt negativa trenden inom EU mot molntjänster lär – om de isolationistiska inslagen sätts i verket – ge dyrare och sämre resultat än vad som annars hade varit möjligt. De stora molntjänstleverantörerna har mycket bättre cybersäkerhet än ett normalt företag. Däremot tror man inte att produktionen och servicen av stand-alone-system kommer att försvinna, så länge det finns företag som är villiga att betala för dem. Sannolikt får vi i stället ett antal hybridlösningar.

Företag 4

FRÅGOR

Omfattning

1. Har ni utsatts för industrispionage (varmed avses olaglig eller obehörig inhämtning av företagshemligheter, oavsett metod)?

   Ja, men såvitt känt inte från någon nationalstat. Det är oetiska konkurrenter som försökt inhämta information.

A. Har ni utsatts för cyberbrottslighet (varmed avses obehörigt intrång i eller sabotage av dataföretagets system)? + frågorna nedan

   Ja

2. Vilket/vilka tillvägagångssätt har använts?

   Phishing-attacker/clickmail/skadlig kod är ofta förekommande. Så kallad portskanning förekommer. Hittills inga DDOS-attacker. Stöld av laptop-datorer tillhöriga företaget är genomförd, med en ganska avancerad metodik.

3. Vilken omfattning och frekvens har denna verksamhet haft?

   Phishing med mera sker dagligen – det är ett ständigt brus.

4. Under hur lång tid har angreppen pågått?

   Phishing pågår ständigt.

5. Vilken sorts information är det som har inhämtats och i vilken form?

   Anbudsunderlag, prissättningsmodeller och databaser.

6. Vilka särskilda konsekvenser bedömer ni att angreppen medfört för ert företag?

   Svårbedömt – för närvarande finns otillräckligt underlag.

7. Hur stora kostnader kan de fullbordade angreppen antas ha medfört i affärsmässigt hänseende?

   Inget direkt känt i detta avseende.

8. Har ni vidtagit några skyddsåtgärder med anledning av angreppen?

   Ja

9. Om ja – vilka skyddsåtgärder?

   Särskild säkerhetsorganisation med cirka 10 personer. CSO rapporterar direkt till vd. Rutiner avsedda att försvåra angrepp eller virus i systemen – ordning och reda i all it-användning är grunden. Externa systemleverantörer anlitas, de har mycket högre kompetens på säkerhetsområdet än ett företag vanligtvis kan vidmakthålla. Företaget kombinerar emellertid därefter deras produkter efter eget huvud. Sandbox-analys av misstänkt skadlig kod.

10. Hur stora kostnader kan skyddsåtgärderna antas ha medfört?

    Cirka 20–25 miljoner kronor/år.

11. Vilka bedömer ni är de mest frekventa aktörerna: konkurrentföretag/främmande makt/kriminella/anställda/annan aktör?

    Kriminella aktörer.

12. Vilka angripare bedömer ni vara mest problematiska/svårast att motverka?

    Kriminella eller andra aktörer som använder så kallad ransomware. Metoden är i sig inte svår att använda, men ger stora skadeverkningar om angriparen lyckas hitta en säkerhetslucka – vare sig detta sker via nätet eller genom att man kommer över en företagsdator med inloggningsuppgifter. Därefter är det enkelt att successivt skaffa sig högre behörigheter och infektera så gott som all it-utrustning.

13. Har ni någon gång vidtagit rättsliga åtgärder för att motverka angrepp?

    Alla brott som upptäcks polisanmäls.

14. Har dessa åtgärder lett till något resultat?

    Nej

15. Hur ser ni på den svenska statens förmåga att skydda svenska företag mot dessa angrepp och att stödja dem avseende påföljande skyddsåtgärder?

    Den är lika med noll.

16. Hur ser ni på EU:s förmåga att skydda och stödja unionens företag i ovan avseende?

    Enisa bidrar med standarder och best practice. Europol är inte att räkna med i detta sammanhang.

17. Vilka statliga policyförändringar skulle ni vilja se avseende bekämpning av industrispionage/cyberbrottslighet?

    Statliga myndigheter vill från tid till annan att företaget ska delge dem sina erfarenheter, men det finns ingen reciprocitet över huvud taget. De ger aldrig några tips tillbaka. Det är främst i Storbritannien och Nederländerna som det finns fungerande samverkan mellan staten och det privata näringslivet – de är goda förebilder. De svenska företagen skulle behöva en form för privat/offentlig samverkan på detta område, där information kan lämnas och mottas utan risk för offentliggörande.

Avslutande kommentar om så kallade molntjänster

Molntjänster är här för att stanna. De kommer bara att öka i betydelse och marknadsandelar. De stora leverantörerna av sådana tjänster har kompetens i världsklass på säkerhetsområdet. Detta företag avser dock att bibehålla on-premises-lösningar för kanske cirka 10 procent av sin datavolym. Det handlar både om säkerhetsklassad information och data som är vitala för företaget av andra anledningar.

Företag 5

FRÅGOR

Omfattning

1. Har ni utsatts för industrispionage (varmed avses olaglig eller obehörig inhämtning av företagshemligheter, oavsett metod)?

   Ja

A. Har ni utsatts för cyberbrottslighet (varmed avses obehörigt intrång i eller sabotage av dataföretagets system)? + frågorna nedan

   Ja

2. Vilket/vilka tillvägagångssätt har använts?

   Phishing-attacker/clickmail/skadlig kod är mycket ofta förekommande. Så kallad portskanning förekommer. Rekrytering av insider. Alla kända metoder för cyberangrepp har använts.

3. Vilken omfattning och frekvens har denna verksamhet haft?

   Phishing sker dagligen.

4. Under hur lång tid har angreppen pågått?

   De pågår ständigt.

5. Vilken sorts information är det som har inhämtats och i vilken form?

   Denna uppgift är för känslig – företaget vill ej uppge ens karaktären av denna information.

6. Vilka särskilda konsekvenser bedömer ni att angreppen medfört för ert företag?

   Ständigt arbete med att bygga upp och vidmakthålla olika former av säkerhetssystem – vi tar inga risker.

7. Hur stora kostnader kan de fullbordade angreppen antas ha medfört i affärsmässigt hänseende?

   Ingen uppgift lämnas.

8. Har ni vidtagit några skyddsåtgärder med anledning av angreppen?

   Ja

9. Om ja – vilka skyddsåtgärder?

   Särskild säkerhetsorganisation på flera nivåer och med olika sorters inriktning. Den egna organisationen har stora resurser och högre kompetens på säkerhetsområdet än ett företag vanligtvis kan vidmakthålla. Traditionellt säkerhetsarbete paras med kontinuerlig hotbildsanalys. Detektering och spårning av angrepp sker dygnet runt. Företagets medarbetare hålls vaksamma genom att man regelbundet producerar och skickar egna så kallade phishing-mejl. Extern kompetens köps in i undantagsfall.

10. Hur stora kostnader kan skyddsåtgärderna antas ha medfört?

    Mycket stora, hundratals miljoner kronor/år.

11. Vilka bedömer ni är de mest frekventa aktörerna: konkurrentföretag/främmande makt/kriminella/anställda/annan aktör?

    Okvalificerade kriminella aktörer.

12. Vilka angripare bedömer ni vara mest problematiska/svårast att motverka?

    Statliga aktörer, med eller utan kriminell täckmantel. Angriparna kan som kollektiv beskrivas som en pyramid, där de flesta och minst kvalificerade utgör pyramidens bas. De mest kvalificerade angriparna antas vara så sofistikerade att de efterlämnar få eller inga spår efter att de inhämtat sökt information, alternativt placerat ut skadlig programkod avsedd att aktiveras i särskilt avsett fall. När kvalificerade aktörer använder sig av spårbar så kallad ransomware ökar dock risken för att tillvägagångssättet ska sprida sig på nätet och kunna utnyttjas av (andra) kriminella.

13. Har ni någon gång vidtagit rättsliga åtgärder för att motverka angrepp?

    Ej svar

14. Har dessa åtgärder lett till något resultat?

    Ej svar

15. Hur ser ni på den svenska statens förmåga att skydda svenska företag mot dessa angrepp och att stödja dem avseende påföljande skyddsåtgärder?

    Den är låg, men man bör beakta att staten inte tagit på sig uppgiften att generellt skydda svenska företag, vare sig mot industrispionage i konventionell mening eller cyberbrottslighet.

16. Hur ser ni på EU:s förmåga att skydda och stödja unionens företag i ovan avseende?

    Sannolikt ingen förmåga alls. Europol har möjligen viss kompetens.

17. Vilka statliga policyförändringar skulle ni vilja se avseende bekämpning av industrispionage/cyberbrottslighet?

    Det finns i Sverige av idag en hög grad av naivitet avseende säkerhetshoten över huvud taget Man bör försöka hitta en modell som överbryggar de hinder som idag finns för delgivning av säkerhetsstärkande information, både inom och mellan myndigheter samt mellan myndigheter och företag. Förvisso finns det kontakter på det personliga planet mellan myndighetspersoner och företagspersoner, som i någon mån botar den bristen. Dessa kontakter är emellertid helt informella och inte sanktionerade från statens sida, och de innebär inte en tillfredsställande lösning på problemet. En möjlig utväg skulle kunna vara att tillsätta en statlig utredning som sker på vetenskaplig grund, där representanter för olika särintressen (statliga, politiska, myndighets- eller näringslivsbaserade) inte ges möjlighet att bestämma utfallet av utredningsresultaten. Den svenska förvaltningsmodellen medför en gordisk knut av låsningar, som hittills hindrat effektiv säkerhetssamverkan mellan staten och näringslivet. Utredningens uppgift vore att försöka hitta en möjlig lösning.

Företag 6

FRÅGOR

Omfattning

1. Har ni utsatts för industrispionage (varmed avses olaglig eller obehörig inhämtning av företagshemligheter, oavsett metod)?

   Nej, inte såvitt känt. Däremot finns det ett antal personer som rör sig i företagets yttre miljö vilka bedöms kunna utgöra potentiella hot. Särskild försiktighet iakttas i förhållande till dem.

A. Har ni utsatts för cyberbrottslighet (varmed avses obehörigt intrång i eller sabotage av dataföretagets system)? + frågorna nedan

   Ja

2. Vilket/vilka tillvägagångssätt har använts?

   Phishing-attacker/clickmail/skadlig kod är mycket ofta förekommande. DDOS-attack. Alla kända metoder för cyberangrepp har använts. Vad man kunnat iaktta under senare tid är att de som använder phishing väsentligt stärkt sin förmåga att producera lockande ”beten”. De arbetar synbarligen uthålligt och med gott grundarbete – research. Man har bland annat använt metoden att först angripa utländska bolag, därefter högt upp i det svenska bolagets hierarki, och med fullständig anpassning till den dygnsrytm som är normal för den interna kommunikationen. I något fall har man lyckats bryta sig in i en mejltråd.

3. Vilken omfattning och frekvens har denna verksamhet haft?

   Phishing sker dagligen – dagligt brus.

4. Under hur lång tid har angreppen pågått?

   De pågår ständigt.

5. Vilken sorts information är det som har inhämtats och i vilken form?

   Såvitt känt har ingen intern information av vikt blivit kompromitterad, men man är ödmjuk inför möjligheten av att det kan ha förekommit – 100-procentig säkerhet finns inte.

6. Vilka särskilda konsekvenser bedömer ni att angreppen medfört för ert företag?

   Ett ständigt arbete med att bygga upp och vidmakthålla olika former av säkerhetssystem. Ett särskilt problem vore om de lyckades att kompromettera företagets interna kommunikation. Den internt ömsesidiga tilltron skulle kunna skadas, vilket sannolikt leder till överförsiktighet och effektivitetsbortfall. Beträffande externa effekter är det av väsentlig betydelse att skydda företagets varumärke.

7. Hur stora kostnader kan de fullbordade angreppen antas ha medfört i affärsmässigt hänseende?

   Ingen uppgift lämnas.

8. Har ni vidtagit några skyddsåtgärder med anledning av angreppen?

   Ja

9. Om ja – vilka skyddsåtgärder?

   Särskild säkerhetsorganisation. AI-baserade verktyg, både med övervakad och oövervakad inlärning för detektering och spårning av angrepp, köps in externt, liksom kapacitet att svara på svårare externa hot/angrepp. Sektionering av intern information.

10. Hur stora kostnader kan skyddsåtgärderna antas ha medfört?

    Ingen uppgift lämnas.

11. Vilka bedömer ni är de mest frekventa aktörerna: konkurrentföretag/främmande makt/kriminella/anställda/annan aktör?

    Kriminella aktörer. Därtill kommer sådana som har föregivit idealistiska syften, som vill sabotera företaget just för att det är stort och därmed i sig anses vara moraliskt illegitimt.

12. Vilka angripare bedömer ni vara mest problematiska/svårast att motverka?

    En insider som planteras i företaget. Därefter insiders som en angripare lyckats plantera i en underleverantör av it-tjänster. Ett särskilt problem just nu är att coronapandemin medfört ett starkt ökat behov av att installera fler digitala arbetsverktyg, vilket i sig ökar komplexiteten i arbetet med att bedöma säkerhetsnivåerna i olika lösningar och hos olika leverantörer.

13. Har ni någon gång vidtagit rättsliga åtgärder för att motverka angrepp?

    Nej

14. Har dessa åtgärder lett till något resultat?

    Ej relevant

15. Hur ser ni på den svenska statens förmåga att skydda svenska företag mot dessa angrepp och att stödja dem avseende påföljande skyddsåtgärder?

    Staten, såvitt man kan bedöma utifrån, besitter hög kompetens på aktuellt område. Den besitter sannolikt också information som det skulle vara av stort värde för svenska företag att kunna ta del av – också i generella termer. Informella kontakter med myndighetsföreträdare ger emellertid vid handen att de känner sig totalt bakbundna av svenska lagar och regler, som förhindrar delgivning. Det skulle behövas någon form av pålitlig ”mäklarinstans”. Storbritannien och Australien har goda exempel på sådant, både avseende individuella företagskontakter och allmän rådgivning. För egen del tvingades företaget vid ett tillfälle att vända sig till myndigheter i Finland för att få hjälp. Den svenska polisen har vare sig tillräcklig kompetens eller resurser i övrigt.

16. Hur ser ni på EU:s förmåga att skydda och stödja unionens företag i ovan avseende?

    Låg. Enisa har viss kompetens.

17. Vilka statliga policyförändringar skulle ni vilja se avseende bekämpning av industrispionage/cyberbrottslighet?

    Det borde kunna gå att åstadkomma en vettig form för samverkan och informationsöverföring som inte bryter mot svensk lag, men ändå ger företag större möjligheter att skydda sig. Goda exempel finns i andra länder. Om inte så kan man ta de svenska bankernas samarbete på säkerhetsområdet som en möjlig utgångspunkt. Därtill kommer att det är oklart huruvida privata svenska ekonomiska intressen beaktas över huvud taget när staten gör bedömningar av vad som är nationellt skyddsvärda intressen – den frågan förtjänar visst övervägande.

Allmän reflektion om så kallade molntjänster

Molntjänsternas intåg i företagen har både positiva och negativa sidor. De överskuggas först och främst av de geopolitiska motsättningarna. På pluskontot kan skrivas effektivare backoffice-tjänster, bättre samverkansmöjligheter, högre fysisk säkerhet, mera datorkraft och allmänt sett större tillgänglighet. På minuskontot finns risken för koncentration till ett mycket litet antal dominerande leverantörer, där det ibland kan vara oklart vem som har äganderätten till informationen, där denna dessutom är krypterad från leverantörsföretaget och där detta företag förfogar över kodnycklarna. I värsta fall kan ett företag stå utan tillgång till sin egen information. Beträffande säkerhetsnivåerna finns det inget som entydigt pekar på att molntjänstleverantörerna har högre åtkomstsäkerhet än vad man själv skulle kunna åstadkomma – givet priset. Tjänsteköpet innebär oftast att köparen dels själv måste definiera och ställa in säkerhetsfunktionerna i produkten, dels måste betala en bra slant mer för de riktigt höga säkerhetsnivåerna. Som alltid handlar det om att göra en avvägning mellan skyddsbehovet och kostnaden.

Företag 7

FRÅGOR

Omfattning

1. Har ni utsatts för industrispionage (varmed avses olaglig eller obehörig inhämtning av företagshemligheter, oavsett metod)?

   Inte såvitt känt, men med tanke på den grad av sofistikering som finns hos en potentiell angripare kan man inte säkert veta.

A. Har ni utsatts för cyberbrottslighet (varmed avses obehörigt intrång i eller sabotage av dataföretagets system)? + frågorna nedan

   Ja

2. Vilket/vilka tillvägagångssätt har använts?

   Phishing-attacker/clickmail är ofta förekommande. Så kallad social engineering är allt mer avancerad (försök att lura interna användare att avslöja företagsintern information, oavsett syftet). Ransomware har förekommit men avvärjts. Man har inte utsatts för DDOS-attacker.

3. Vilken omfattning och frekvens har denna verksamhet haft?

   Dagligt brus, men man bedömer sig sällan vara den direkta måltavlan. Man är föremål för de mängdangrepp som kriminella utför på måfå.

4. Under hur lång tid har angreppen pågått?

   De pågår ständigt.

5. Vilken sorts information är det som har inhämtats och i vilken form?

   Total säkerhet finns inte, men såvitt man vet har ingen vital information inhämtats.

6. Vilka särskilda konsekvenser bedömer ni att angreppen medfört för ert företag?

   Fortlöpande arbete med att bygga upp och vidmakthålla olika former av säkerhetssystem och rutiner. Ett dataläckage inträffade för ett antal år sedan.

7. Hur stora kostnader kan de fullbordade angreppen antas ha medfört i affärsmässigt hänseende?

   Ej relevant

8. Har ni vidtagit några skyddsåtgärder med anledning av angreppen?

   Ja

9. Om ja – vilka skyddsåtgärder?

   Organisation avseende säkerhetsåtgärderna är integrerad i it-verksamheten. Multifaktoridentifiering införd. Rutiner och utbildning. Företaget bedömer sig inte vara direkt intressant för en avancerad angripare.

10. Hur stora kostnader kan skyddsåtgärderna antas ha medfört?

    50–100 miljoner kronor/år. Definitionen av vad som avses gör bedömningen svår.

11. Vilka bedömer ni är de mest frekventa aktörerna: konkurrentföretag/främmande makt/kriminella/anställda/annan aktör?

    Kriminella aktörer, innefattande så kallade script kids (tonåriga hackare). Sedan kommer aktörer med föregivet idealistiska syften, som kan vilja sabotera företaget.

12. Vilka angripare bedömer ni vara mest problematiska/svårast att motverka?

    En främmande makt, med eller utan mellanhand i form av kriminell aktör, därefter kriminella aktörer och sist en insider.

13. Har ni någon gång vidtagit rättsliga åtgärder för att motverka angrepp?

    Nej, inte i egentlig mening. Polisanmälan har gjorts i enstaka fall.

14. Har dessa åtgärder lett till något resultat?

    Nej

15. Hur ser ni på den svenska statens förmåga att skydda svenska företag mot dessa angrepp och att stödja dem avseende påföljande skyddsåtgärder?

    Den är otillräcklig. De informella kontakter som kan förekomma är otillräckliga för att bota den bristen. För många företag finns det ett stort behov av att staten tillgängliggör både allmän information och rekommendationer/riktlinjer för it-säkerhet.

16. Hur ser ni på EU:s förmåga att skydda och stödja unionens företag i ovan avseende?

    Obekant

17. Vilka statliga policyförändringar skulle ni vilja se avseende bekämpning av industrispionage/cyberbrottslighet?

    Se svar på fråga 15. Det viktigaste kanske vore att staten/politiken börjar inse räckvidden och konsekvenserna av de lagstiftningsbeslut som fattas – både på EU-nivå och nationell nivå. GDPR är ett exempel på detta, som medfört enorma kostnader för näringslivet.

Allmän reflektion om så kallade molntjänster

Företaget har en pragmatisk syn på molntjänster. De är kostnadseffektiva och medger större flexibilitet för mobila användare. Det gamla paradigmet med in-house-lösningar håller på att bli irrelevant. Det som är viktigt är att skydda identiteter och information. Man följer GDPR. Cirka 80 procent av de nya it-lösningar som introduceras är molnbaserade. Företaget bedömer sig för närvarande inte vara utsatt för risk att intern information därigenom kompromitteras, på grund av konkurrenters eller främmande makts intressen. Risken för att bli utelåst från sin egen information bedöms vara mycket obetydlig. Emellertid anser man att molntjänsterna fortfarande är relativt tekniskt omogna – de erbjuder för närvarande inte de högst ställda kraven på säkerhet.

Företag 8

FRÅGOR

Omfattning

1. Har ni utsatts för industrispionage (varmed avses olaglig eller obehörig inhämtning av företagshemligheter, oavsett metod)?

   Ej såvitt känt, men försök sker – se nedan.

A. Har ni utsatts för cyberbrottslighet (varmed avses obehörigt intrång i eller sabotage av dataföretagets system)? + frågorna nedan

   Ja

2. Vilket/vilka tillvägagångssätt har använts?

   Phishing är mycket ofta förekommande – tillvägagångssätten blir allt mer sofistikerade. Ransomware har förekommit. DDOS-attacker pågår kontinuerligt. Försök till åtkomst av företagets AD (active directory) pågår kontinuerligt.

3. Vilken omfattning och frekvens har denna verksamhet haft?

   Det är ett ständigt brus av stor omfattning. Man är föremål för de mängdangrepp som kriminella utför på måfå.

4. Under hur lång tid har angreppen pågått?

   De pågår ständigt. Attacken mot företagets AD har pågått i åtminstone tre år.

5. Vilken sorts information är det som har inhämtats och i vilken form?

   Försök pågår ständigt att inhämta kunddata, av alla de slag, för vidare exploatering.

6. Vilka särskilda konsekvenser bedömer ni att angreppen medfört för ert företag?

   Säkerhetssystem, rutiner och kontinuerlig utbildning måste byggas upp och vidmakthållas. Information har vid vissa tillfällen läckt ut till det så kallade darknet, där en enskilds persondata kan köpas för 5 euro.

7. Hur stora kostnader kan de fullbordade angreppen antas ha medfört i affärsmässigt hänseende?

   Ingen uppgift. Ransomware-attacken kostade cirka 5 miljoner kronor att åtgärda.

8. Har ni vidtagit några skyddsåtgärder med anledning av angreppen?

   Ja

9. Om ja – vilka skyddsåtgärder?

   Organisation avseende säkerhetsåtgärderna är integrerad i it-verksamheten. Rutiner och utbildning. Inköp av skydd mot DDOS-attacker, kryptering av all extern kommunikation och viss del av den interna. Anomalidetektering sker kontinuerligt. Anlitande av både internt och externt så kallat red team (auktoriserad angripare som söker efter svagheter i systemen) och så kallad bug bounty (belöning för extern aktör som upptäcker säkerhetsbrister).

10. Hur stora kostnader kan skyddsåtgärderna antas ha medfört?

    Definitionen av vad som avses gör bedömningen svår, men man uppskattar de direkta kostnaderna för denna del av säkerhetsorganisationen till cirka 25 miljoner kronor/år i personalkostnader och cirka 25 miljoner kronor/år i investeringskostnader.

11. Vilka bedömer ni är de mest frekventa aktörerna: konkurrentföretag/främmande makt/kriminella/anställda/annan aktör?

    Kriminella aktörer. I det egna fallet med den fortgående attacken mot AD bedömer man att den härrör från en statlig aktör i Kina, en bedömning som delas av andra företag.

12. Vilka angripare bedömer ni vara mest problematiska/svårast att motverka?

    En främmande makt, därefter kriminell aktör. Skillnaden i kompetensnivå dem emellan bedöms numera vara liten – samma tillvägagångssätt, samma teknik och (sannolikt) samma personer används i bådas syften.

13. Har ni någon gång vidtagit rättsliga åtgärder för att motverka angrepp?

    Nej

14. Har dessa åtgärder lett till något resultat?

    Ej relevant

15. Hur ser ni på den svenska statens förmåga att skydda svenska företag mot dessa angrepp och att stödja dem avseende påföljande skyddsåtgärder?

    Den är lika med noll. Polisen har vare sig resurser eller kompetens för att hantera industrispionage/cyberangrepp. I utlandet har företaget fått stöd från NCSC (National Cyber Security Centre) i Storbritannien, och i USA från FBI.

16. Hur ser ni på EU:s förmåga att skydda och stödja unionens företag i ovan avseende?

    Ingen kännedom. Enskilda medlemsstater har vissa resurser.

17. Vilka statliga policyförändringar skulle ni vilja se avseende bekämpning av industrispionage/cyberbrottslighet?

    Storbritannien och i viss mån Nederländerna är mycket bättre än Sverige på att hjälpa och stödja sina företag. Det borde kunna gå att skapa ett nationellt, statligt, cyberteam för att hjälpa till vid allvarliga angrepp. Samverkan med företagen borde vara obligatoriskt – det är de som vet vad som pågår. Phishing och DDOS-attacker är vardagsmat – den stora oron man hyser i företaget är om det skulle lyckas att kompromettera DNS-systemet (internets ”telefonkatalog”).

Allmän reflektion om så kallade molntjänster

Det är en utmaning att förhålla sig till molntjänster – man måste hela tiden överväga kostnaderna i förhållande till effekten. Deras effektivitet för att bedriva affärer är hundra gånger större än vad ett enskilt företag skulle kunna bygga upp. Molntjänsterna har efter hand uppnått mycket bättre säkerhetsnivåer än vad som ursprungligen erbjöds. Det finns emellertid svagheter – man kan inte vara säker på att den säkerhetsnivå man köpt faktiskt motsvaras av vad som levereras. Det medför ett ständigt arbete med att kontrollera och utvärdera köpta tjänster. Förvisso finns det ännu små delar av verksamheten som är så att säga lokalt baserade, men det finns tvivel om hur länge man kan stanna kvar i sådana system.

Företag 9

FRÅGOR

Omfattning

1. Har ni utsatts för industrispionage (varmed avses olaglig eller obehörig inhämtning av företagshemligheter, oavsett metod)?

   Ja

A. Har ni utsatts för cyberbrottslighet (varmed avses obehörigt intrång i eller sabotage av dataföretagets system)? + frågorna nedan

   Ja

2. Vilket/vilka tillvägagångssätt har använts?

   Phishing och så kallad spear phishing är mycket ofta förekommande. Så kallad spoofing där man utger sig för att vara en kollega eller samarbetspartner förekommer. Ransomware har förekommit hos partnerföretag. Så kallad portskanning förekommer.

3. Vilken omfattning och frekvens har denna verksamhet haft?

   Det pågår hela tiden, men frekvensen ökar.

4. Under hur lång tid har angreppen pågått?

   De pågår ständigt.

5. Vilken sorts information är det som har inhämtats och i vilken form?

   I första hand försöker man ladda in så kallad ransomware (kryptering av företagets information) i företagets system för utpressningsförsök; mer avancerade angripare försöker dessutom ladda ner företagets information externt, både i utpressningssyfte och för att kunna sälja vidare. Den information som främst söks är forskningsdata och produktinformation.

6. Vilka särskilda konsekvenser bedömer ni att angreppen medfört för ert företag?

   Ingen uppgift.

7. Hur stora kostnader kan de fullbordade angreppen antas ha medfört i affärsmässigt hänseende?

   Ingen uppgift.

8. Har ni vidtagit några skyddsåtgärder med anledning av angreppen?

   Ja

9. Om ja – vilka skyddsåtgärder?

   En omfattande säkerhetsorganisation är uppbyggd. Rutiner förfinas. Kontinuerlig utbildning och vaksamhetskampanj. Utsändande av egna phishing-mejl för att öka vaksamheten. Externt inköp av hotbildsanalys och varningsflaggor – cirka 4000 exempel på skadlig kod spärras i företagets it-system varje månad. Anomalidetektering sker kontinuerligt, bland annat i form av så kallade user behaviour analytics (automatisk analys för att upptäcka onaturlig användning av it-system,

till exempel plötslig ökning av nedladdningsvolym). Man bedömer sig vara i framkant avseende it-säkerhet för ett företag som inte befinner sig i branschen.

10. Hur stora kostnader kan skyddsåtgärderna antas ha medfört?

    Definitionen påverkar bedömningen. Under alla omständigheter handlar det om hundratals miljoner kronor per år.

11. Vilka bedömer ni är de mest frekventa aktörerna: konkurrentföretag/främmande makt/kriminella/anställda/annan aktör?

    Kriminella aktörer är vanligast, men man utsätts också för frekventa angrepp från vad som bedöms vara statliga aktörer.

12. Vilka angripare bedömer ni vara mest problematiska/svårast att motverka?

    Det är för närvarande svårt att skilja kriminella från stater – båda har likartad kompetens, och kriminella grupperingar används av stater. Man måste inse att det inte längre handlar om tonåriga hackare, utan om proffs som ingår i stora kriminella organisationer som bedriver it-angrepp i industriell skala.

13. Har ni någon gång vidtagit rättsliga åtgärder för att motverka angrepp?

    Ja

14. Har dessa åtgärder lett till något resultat?

    Ja – men inte i Sverige. Bland annat i USA genom FBI.

15. Hur ser ni på den svenska statens förmåga att skydda svenska företag mot dessa angrepp och att stödja dem avseende påföljande skyddsåtgärder?

    Den är minimal. I USA har företaget fått stöd från CISA (Cybersecurity & Infrastructure Security Agency) och i Storbritannien från NCSC (National Cyber Security Centre).

16. Hur ser ni på EU:s förmåga att skydda och stödja unionens företag i ovan avseende?

    Den har blivit bättre men är fortfarande minimal.

17. Vilka statliga policyförändringar skulle ni vilja se avseende bekämpning av industrispionage/cyberbrottslighet?

    I Sverige är Säkerhetspolisen bara intresserad av det som anses vara hot mot rikets säkerhet – vanliga företag kan inte förvänta sig något stöd därifrån.

    Man borde efterlikna det tyska exemplet, där den federala myndigheten BSI (Bundesamt für Sicherheit in der Informationstechnik) gör en analys av vilka företag som utgör en del av den kritiska infrastrukturen. Därefter får de rekommendationer om nödvändig skyddsnivå, och kan få varningsflaggor, råd och information. CISA i USA och NCSC i Storbritannien är också bra exempel på vad man kan göra för att stötta företag. Sverige borde kunna samarbeta med de nämnda länderna på det här området, till exempel genom att identifiera vilka statsaktörer som ligger bakom angrepp. Nu finns ingen svensk statlig beredskap avseende it-angrepp, och precis som covid-19 har visat att Sverige saknade beredskap på pandemiområdet så lär det förr eller senare visa sig negativa konsekvenser också på it-området. De flesta svenska företag har ingen att vända sig till.

Allmän reflektion om så kallade molntjänster

Molntjänster ökar säkerheten totalt sett – det är bättre med flera ”öar” av information än att förlita sig på sin egen skyddsmur. Det är ett misstag att tro att man skulle kunna säkra sig genom att låsa in informationen inom företaget eller nationellt.

Företag 10

FRÅGOR

Omfattning

1. Har ni utsatts för industrispionage (varmed avses olaglig eller obehörig inhämtning av företagshemligheter, oavsett metod)?

   Nej, inte i konventionell mening

A. Har ni utsatts för cyberbrottslighet (varmed avses obehörigt intrång i eller sabotage av dataföretagets system)? + frågorna nedan

   Ja

2. Vilket/vilka tillvägagångssätt har använts?

   Phishing och så kallad spear phishing är ofta förekommande. Metoderna blir allt mer förfinade – med korrekt språk utan stavfel, och med företagets egna grafiska mallar som förebild. Att utge sig för att vara en kollega eller samarbetspartner förekommer, också vid telefonsamtal. Ransomware har förekommit i enstaka fall. Så kallad portskanning förekommer. Man kartlägger organisationen för att hitta personer ett par nivåer under den högsta ledningsnivån, oftast på finans- eller HR-sidan. Storskaliga attacker pågår, men såvitt känt har inga stora säkerhetsläckor förekommit. Man har inte varit utsatt för DDOS-attacker, däremot förekommer försök att kompromettera Teams-funktionen.

3. Vilken omfattning och frekvens har denna verksamhet haft?

   Den pågår kontinuerligt, men frekvensen ökar. Företagets system blockerar cirka 40 000 specifika hot per månad, och registrerar cirka 18–19 miljoner angreppsförsök per månad. Sedan covid-19 började har angreppen ökat med mellan 100 och 150 procent.

4. Under hur lång tid har angreppen pågått?

   De pågår ständigt.

5. Vilken sorts information är det som har inhämtats och i vilken form?

   I första hand information som kan användas i bedrägligt syfte. Så vitt företaget känner till har angrepp inte skett i syfte att inhämta produktinformation eller kurspåverkande information.

6. Vilka särskilda konsekvenser bedömer ni att angreppen medfört för ert företag?

   Eftersom kunderna förväntar sig allt fler digitala funktioner inbäddade i produkterna, som kan användas via molntjänster, måste företaget i allt större

utsträckning beakta säkerhetsaspekterna. Därtill kommer att man tvingas bygga in fyrfaldiga kontrollmekanismer i till exempel finansiella processer. Angreppen genererar en automatisk misstro i den digitala kommunikationen som försvårar verksamheten.

7. Hur stora kostnader kan de fullbordade angreppen antas ha medfört i affärsmässigt hänseende?

   Ej relevant.

8. Har ni vidtagit några skyddsåtgärder med anledning av angreppen?

   Ja

9. Om ja – vilka skyddsåtgärder?

   En säkerhetsorganisation är uppbyggd. Ett flertal tekniska skydd finns inbyggda i it-systemen: brandväggar, virusskydd etc. Man bedömer sig ligga på en säkerhetsnivå som är anpassad efter sin verksamhet och de interna användarnas behov – normal industriproduktion som inte anses vara samhällskritisk.

10. Hur stora kostnader kan skyddsåtgärderna antas ha medfört?

    Ingen uppgift kan lämnas, bland annat på grund av definitionssvårigheter.

11. Vilka bedömer ni är de mest frekventa aktörerna: konkurrentföretag/främmande makt/kriminella/anställda/annan aktör?

    Kriminella aktörer är vanligast. Man har inte sett några tecken på angrepp från konkurrenter eller främmande makt.

12. Vilka angripare bedömer ni vara mest problematiska/svårast att motverka?

    De man inte har sett. En statlig eller statsunderstödd aktör bedömer man sig inte ha resurser att möta.

13. Har ni någon gång vidtagit rättsliga åtgärder för att motverka angrepp?

    Ja. Allt härledningsbart polisanmäls.

14. Har dessa åtgärder lett till något resultat?

    Nej

15. Hur ser ni på den svenska statens förmåga att skydda svenska företag mot dessa angrepp och att stödja dem avseende påföljande skyddsåtgärder?

    Man vet egentligen inte, eftersom man inte anses ingå i den kritiska infrastrukturen och därmed inte har anledning att ha kontakt med statliga myndigheter i säkerhetsfrågor.

16. Hur ser ni på EU:s förmåga att skydda och stödja unionens företag i ovan avseende?

    Ingen uppfattning, men det står klart att GDPR liksom motsvarande lagstiftningar i andra länder lägger en stor börda på företagen.

17. Vilka statliga policyförändringar skulle ni vilja se avseende bekämpning av industrispionage/cyberbrottslighet?

Internet kan liknas vid vilda västern, men oaktat de integritetsskyddsrelaterade aspekterna av nätfriheten så borde en ökad grad av övervakning kunna ske. För närvarande sker såvitt känt inget överstatligt samarbete för att motverka den globala cyberbrottsligheten – det borde kunna åstadkommas.

Allmän reflektion om så kallade molntjänster

Molntjänsterna är bra och behövs för att företaget ska kunna bedriva sin världsomspännande verksamhet. Därtill kommer att kunderna i allt större utsträckning kräver inbäddning av it-system som kan användas och servas via molnet.

Företag 11

FRÅGOR

Omfattning

1. Har ni utsatts för industrispionage (varmed avses olaglig eller obehörig inhämtning av företagshemligheter, oavsett metod)?

Nej, inte såvitt känt.

A. Har ni utsatts för cyberbrottslighet (varmed avses obehörigt intrång i eller sabotage av dataföretagets system)? + frågorna nedan

Ja

2. Vilket/vilka tillvägagångssätt har använts?

Phishing förekommer ofta, med tillhörande försök att plantera in skadlig kod. Betena blir allt mer trovärdiga. För ett antal år sedan lyckades en angripare ta sig in i en mejltjänst som då enbart hade enfaktorautentisering. Så kallad portskanning förekommer, men försöken att ta sig in har misslyckats. Man har inte utsatts för DDOS-attacker eller försök att ta sig in i Teams. Man har inte varit föremål för så kallad ransomware eller annan utpressning.

3. Vilken omfattning och frekvens har denna verksamhet haft?

Det sker ständiga intrångsförsök. Företaget har statistik sedan 2013, och mängden angrepp har uppvisat en något fallande trend sedan dess. Dock ser man nu en uppgång sedan sommaren. Cirka 200 000 phishing-mejl med tillhörande skadlig kod neutraliseras per månad.

4. Under hur lång tid har angreppen pågått?

De pågår ständigt. Man bedömer sig ej vara särskilt utsatt, utan blir en måltavla för de massangrepp som kriminella företar.

5. Vilken sorts information är det som har inhämtats och i vilken form?

Underlag för olika sorters bedrägeriförsök, ”stöld” av mejl. Angriparna kartlägger uppenbarligen företagets organisation i sådana syften.

6. Vilka särskilda konsekvenser bedömer ni att angreppen medfört för ert företag?

   Ej relevant. Man anser att riktade angrepp i första hand sker mot myndigheter och i andra hand mot företag med kända varumärken.

7. Hur stora kostnader kan de fullbordade angreppen antas ha medfört i affärsmässigt hänseende?

   Ej relevant.

8. Har ni vidtagit några skyddsåtgärder med anledning av angreppen?

   Ja

9. Om ja – vilka skyddsåtgärder?

   En säkerhetsorganisation med ett tiotal medarbetare finns på plats. Man använder sig av sedvanliga verktyg som 2:a generationens brandväggar (med anomalidetektion), virusskydd och skyddad mejl. Man har ett särskilt team som går in och värderar, och vid behov åtgärdar, onormala beteenden eller konstigheter i systemen. Man har köpt in en så kallad red team-tjänst från en extern leverantör (auktoriserad angripare). En del medarbetare låter sig luras av deras mejl, men vad man sett hittills fångar systemens skyddsfunktioner upp skadlig kod. Man tillämpar ISO 27000-standarden för it-säkerhet.

10. Hur stora kostnader kan skyddsåtgärderna antas ha medfört?

    Ingen uppgift kan lämnas. Säkerhetsfunktionerna ingår i så många olika verksamhetsgrenar att en samlad bedömning inte kan göras.

11. Vilka bedömer ni är de mest frekventa aktörerna: konkurrentföretag/främmande makt/kriminella/anställda/annan aktör?

    Kriminella aktörer.

12. Vilka angripare bedömer ni vara mest problematiska/svårast att motverka?

    Den som har insyn i systemets svagheter – oavsett orsaken till att den kunskapen finns.

13. Har ni någon gång vidtagit rättsliga åtgärder för att motverka angrepp?

    Nej. Däremot anmäler man angrepp till banker och internetserviceleverantörer, och personuppgiftsincidenter till Datainspektionen.

14. Har dessa åtgärder lett till något resultat?

    Ej relevant.

15. Hur ser ni på den svenska statens förmåga att skydda svenska företag mot dessa angrepp och att stödja dem avseende påföljande skyddsåtgärder?

    Det finns på övergripande nivå inget stöd att hämta där. För att få polisen att agera över huvud taget så krävs det en personlig kontakt. Det verksamma för ett storföretag är att ingå i det företagsfinansierade säkerhetsforumet ISF (Information Security Forum). I övrigt köper man tjänster från Gartner Group.

16. Hur ser ni på EU:s förmåga att skydda och stödja unionens företag i ovan avseende?

    Man följer Enisa för att kunna urskilja trender, i övrigt inget.

17. Vilka statliga policyförändringar skulle ni vilja se avseende bekämpning av industrispionage/cyberbrottslighet?

    Att även företag som inte bedöms leverera samhällskritisk infrastruktur skulle kunna ha någonstans att vända sig till inom landet.

Allmän reflektion om så kallade molntjänster

För en 8–9 år sedan hade man en skeptisk attityd till molntjänster. Den har ändrats helt – att så långt som möjligt använda molntjänster har blivit en strategi. Man kan köpa säkerhetsnivåer i molnet, till exempel hos Microsoft, men man litar inte helt på det företagets förmåga utan skaffar sig kompletterande skydd mot skadlig kod från specialiserade leverantörer som man bedömer att Microsoft inte kan konkurrera med. Farhågor för att stater skulle kunna skaffa sig insyn i företagets data är irrelevanta – vill de det så kan de. Företagets affärsmodell bygger inte på high-tech utan på andra faktorer.

Företag 12

FRÅGOR

Omfattning

1. Har ni utsatts för industrispionage (varmed avses olaglig eller obehörig inhämtning av företagshemligheter, oavsett metod)?

   Ja

A. Har ni utsatts för cyberbrottslighet (varmed avses obehörigt intrång i eller sabotage av dataföretagets system)? + frågorna nedan

   Ja

2. Vilket/vilka tillvägagångssätt har använts?

   Phishing (cirka 99 procent, men varierar mellan de enkla till avancerade försöken) och ransomware är förekommande. Så kallad portskanning förekommer. Så kallad malware ökar. För ett antal år sedan lyckades en angripare till liten del ta sig in via ett enfaktoridentifieringssystem. Vid ett tillfälle gjordes försök till åtkomst i syfte att använda företagets datorkraft för så kallad bitcoin mining. Så fort en svaghet blir känd på nätet så utsätts man för angrepp via den vektorn. Man har inte utsatts för DDOS-attacker eller försök att ta sig in i Teams. Dock finns viss tveksamhet avseende Microsofts tvåfaktoridentifieringssystem för Teams – den har vissa svagheter. Man har varit utsatt för det så kallade Cloud Hopper-angreppet.

3. Vilken omfattning och frekvens har denna verksamhet haft?

   Den är konstant. Skyddssystemen stoppar cirka 100 000 phishing-mejl per månad, varav cirka 1 500–2 000 bedöms vara mer kvalificerade. Så kallad malware ökar. Ett tiotal phishing-mejl anmäls per vecka av medarbetare.

4. Under hur lång tid har angreppen pågått?

   De pågår ständigt. Med avseende på Cloud Hopper årslångt.

5. Vilken sorts information är det som har inhämtats och i vilken form?

   Man försöker komma åt lösenord, konton och filer. I det sistnämnda avseendet ser man ett särskilt intresse för strategier och pågående utvecklingsarbete.

6. Vilka särskilda konsekvenser bedömer ni att angreppen medfört för ert företag?

   Det är mycket svårbedömt – ej bestämd uppgift.

7. Hur stora kostnader kan de fullbordade angreppen antas ha medfört i affärsmässigt hänseende?

   Ingen uppgift lämnas.

8. Har ni vidtagit några skyddsåtgärder med anledning av angreppen?

   Ja

9. Om ja – vilka skyddsåtgärder?

   En säkerhetsorganisation med ett tiotal medarbetare finns. Därtill bedöms cirka ett trettiotal arbetskrafter vara engagerade hos underleverantörer. Introduktionsutbildning av nyanställda och nätbaserad repetition. Medvetenheten hos medarbetarna har ökat. Företaget har byggt upp något som man beskriver som ett djupförsvar, där skyddsfunktionerna ska medge också decentraliserad användning. Viss anomalidetektering sker. Man har inte använt sig av så kallad bug bounty, men däremot köps så kallad red team-verksamhet in från externa leverantörer. I det sistnämnda fallet ger man ibland uppdrag att angripa företaget i allmänhet, och ibland att försöka tränga in i ett specifikt system.

10. Hur stora kostnader kan skyddsåtgärderna antas ha medfört?

    De direkta kostnaderna bedöms ligga på 40–50 miljoner kronor/år. Skyddsfunktionerna är en integrerad del i så många olika system att en samlad bedömning inte kan göras.

11. Vilka bedömer ni är de mest frekventa aktörerna: konkurrentföretag/främmande makt/kriminella/anställda/annan aktör?

    Nyfikna hackare och kriminella. I fallet Cloud Hopper misstänks Kina vara upphovet.

12. Vilka angripare bedömer ni vara mest problematiska/svårast att motverka?

    En insider. Därutöver kvalificerade kriminella eller stater. Skillnaden dem emellan består i att staters angrepp bedöms vara mycket mer uthålliga.

13. Har ni någon gång vidtagit rättsliga åtgärder för att motverka angrepp?

    Nej

14. Har dessa åtgärder lett till något resultat?

    Ej relevant.

15. Hur ser ni på den svenska statens förmåga att skydda svenska företag mot dessa angrepp och att stödja dem avseende påföljande skyddsåtgärder?

    Det är ömsom vin och ömsom vatten. Säkerhetspolisen bryr sig bara om hot mot rikets säkerhet och huruvida det kan anses vara en statsunderstödd angripare. Därifrån har man blivit bättre på att informera om hot under senare år, men problemet är att den är för generell för att medge relevanta skyddsåtgärder. Man förstår att Säpo vill skydda sina källor, men det innebär att effekten av den information som lämnas ofta uteblir. Därtill är Säpos kontaktmetoder ålderdomliga och ineffektiva. I USA är FBI betydligt mer aktivt. Man anser att hela frågan faller mellan stolarna i Sverige – ingen myndighet har något direkt ansvar.

16. Hur ser ni på EU:s förmåga att skydda och stödja unionens företag i ovan avseende?

    Ingen insikt. Man följer inte Enisas verksamhet.

17. Vilka statliga policyförändringar skulle ni vilja se avseende bekämpning av industrispionage/cyberbrottslighet?

    Det behövs en högre nivå på förtroendet från ansvariga myndigheter gentemot företagen – stora svenska företag har väl så starka skäl att skydda sin verksamhet som staten att skydda Sverige. Man har dock för närvarande inget svar på frågan hur det i så fall borde se ut.

Allmän reflektion om så kallade molntjänster

Säkerheten i en molntjänst är helt avhängig av vem som är leverantör. Generellt sett kan man dock anse att säkerheten blir bättre än att företag ska snickra ihop egna så kallade on-prem-lösningar. Trenden att använda molntjänster är nu så kraftig att den sannolikt inte kommer att kunna stoppas. Problemet med detta är att det ger fler kontaktvägar som ökar sannolikheten för fler felkällor med ty följande risker. Emellertid bör man undvika att lägga precis allting i molnet. Om man tar Microsoft som ett exempel borde man akta sig för att lägga saker i deras moln om man vore i försvarsmaterielbranschen och hade en stor affär på gång när det fanns amerikanska konkurrenter.

Företag 13

FRÅGOR

Omfattning

1. Har ni utsatts för industrispionage (varmed avses olaglig eller obehörig inhämtning av företagshemligheter, oavsett metod)?

   Ja

A. Har ni utsatts för cyberbrottslighet (varmed avses obehörigt intrång i eller sabotage av dataföretagets system)? + frågorna nedan

   Ja

2. Vilket/vilka tillvägagångssätt har använts?

   Beträffande industrispionage det så kallade Cloud Hopper. Phishing är mycket vanligt. Angripare försöker att hacka sig in i företagets it-infrastruktur, direkt eller via företagets leverantörer eller kunder. Alla webbaserade system utsätts för försök att utnyttja svagheter. Inbrott i interna mejltrådar har skett. Ett par mindre försök till förekom för ett antal år sedan men kunde hanteras. Inbrott i mejltrådar sker.

3. Vilken omfattning och frekvens har denna verksamhet haft?

   Den pågår hela tiden. Cirka ett angrepp i veckan lyckas och blir ett utredningsärende. Vanligtvis handlar det om bedrägeri som gör att företaget betalar falska fakturor.

4. Under hur lång tid har angreppen pågått?

   De pågår ständigt. Med avseende på Cloud Hopper årslångt.

5. Vilken sorts information är det som har inhämtats och i vilken form?

   Förutom bedrägeriförsöken handlar det om att försöka få insyn i företagets innovations- och affärsprocesser. Beträffande produktdata bedömer man att det efter hand har blivit mindre intressant – dels på grund av att en konkurrent alltid kan efterapa en produkt med så kallad reverse engineering, dels på grund av att företaget alltid har nya produkter som man anser vara bättre och kan sätta i produktion snabbt.

6. Vilka särskilda konsekvenser bedömer ni att angreppen medfört för ert företag?

   Ingen uppgift kan lämnas.

7. Hur stora kostnader kan de fullbordade angreppen antas ha medfört i affärsmässigt hänseende?

   Det är mycket svårbedömt – ej bestämd uppgift. Fakturabedrägerierna kostar miljonbelopp årligen.

8. Har ni vidtagit några skyddsåtgärder med anledning av angreppen?

   Ja

9. Om ja – vilka skyddsåtgärder?

   En säkerhetsorganisation med ett femtontal medarbetare är uppbyggd. Därtill bedöms ett femtontal årsarbeten vara engagerade hos underleverantörer. Sedan några år tillbaka anser man sig ha förbättrat it-säkerheten avsevärt, både på grund av ökade investeringar på området och på grund av förbättrade rutiner. Alla sedvanliga tekniska skyddsåtgärder har vidtagits. Nätverk har segmenterats och användarbehörigheter har rangordnats. Användningen av Teams är underkastad särskilda skyddsåtgärder. Man använder sig inte av så kallad bug bounty – företagets exponering mot nätet är inte så stor som hos en del andra företag. Man har viss egen förmåga att utföra fingerade angrepp, i övrigt köps den tjänsten in. Man har egen förmåga till incidenthantering.

10. Hur stora kostnader kan skyddsåtgärderna antas ha medfört?

    Ingen uppgift. Emellertid anser man sig hela tiden ligga efter med avseende på potentiella angripare – ständiga nyinvesteringar och rutinförändringar krävs för att hålla någorlunda jämna steg med den tekniska utvecklingen.

11. Vilka bedömer ni är de mest frekventa aktörerna: konkurrentföretag/främmande makt/kriminella/anställda/annan aktör?

    Utan tvekan kriminella.

12. Vilka angripare bedömer ni vara mest problematiska/svårast att motverka?

    En främmande makt. I ett sådant fall bedöms att den skulle lyckas ta sig in i företagets system förr eller senare.

13. Har ni någon gång vidtagit rättsliga åtgärder för att motverka angrepp?

    Det som kan polisanmälas polisanmäls både i Sverige och utomlands. På grund av risken för att avslöja företagshemligheter är dock den utvägen ibland stängd.

14. Har dessa åtgärder lett till något resultat?

    Nej, generellt sett. Dock nämns FBI i USA som ett positivt exempel avseende respons och stöd.

15. Hur ser ni på den svenska statens förmåga att skydda svenska företag mot dessa angrepp och att stödja dem avseende påföljande skyddsåtgärder?

    Den är enormt dålig. FRA och Säpo bryr sig bara om rikets säkerhet, och den information man delger är omgärdad av alltför mycket hysch-hysch. Öppenheten är otillräcklig.

16. Hur ser ni på EU:s förmåga att skydda och stödja unionens företag i ovan avseende?

    Den är låg. Enisas verksamhet är en besvikelse och det saknas ett helhetsgrepp.

17. Vilka statliga policyförändringar skulle ni vilja se avseende bekämpning av industrispionage/cyberbrottslighet?

    Titta på USA! Där finns lagstiftat vilka säkerhetsstandarder som måste vara uppnådda för att man ska anses vara en tillförlitlig leverantör i vissa situationer. Därtill kommer att i stort sett samma krav ställs av många kunder och leveran-

törer och villkoras för att företaget ska kunna vara registrerat på Nasdaq-börsen. Svenska företag kommer i framtiden att behöva likartade riktlinjer för att möta kraven från investerare och kunder. Det behövs också ett forum där ett förtroendefullt utbyte av information avseende best practice kan ske – både på ledningsnivå och säkerhetsspecialistnivån.

Allmän reflektion om så kallade molntjänster

Debatten avseende molntjänster rör ett politiskt krig avsett att tillgodose nationella intressen. De risker som påtalas är i många fall mycket överdrivna, och man bortser från att telemetridata hela tiden laddas ner till systemleverantörernas servrar, oavsett vilka de är. Förståelse saknas för teknologins realiteter. Ur ett företags synvinkel handlar det om att bedöma risken för informationsläckage som vilken annan affärsrisk som helst.

Företag 14

FRÅGOR

Omfattning

1. Har ni utsatts för industrispionage (varmed avses olaglig eller obehörig inhämtning av företagshemligheter, oavsett metod)?

   Nej, inte såvitt känt.

A. Har ni utsatts för cyberbrottslighet (varmed avses obehörigt intrång i eller sabotage av dataföretagets system)? + frågorna nedan

   Ja

2. Vilket/vilka tillvägagångssätt har använts?

   Så kallad spear phishing syftande till fakturabedrägerier. Man är såvitt känt inte utsatt för hackning, och har ej utsatts för DDOS-attacker. Däremot har så kallad portskanning ökat under pandemin när allt fler arbetar hemifrån. Inbrott i interna e-posttrådar har förekommit.

3. Vilken omfattning och frekvens har denna verksamhet haft?

   Flera gånger/vecka eller så gott som dagligen. 90 procent av alla angrepp sker via länkar i e-post.

4. Under hur lång tid har angreppen pågått?

   I någon form har detta pågått sedan digitaliseringen inleddes, men de har eskalerat i omfattning under de sista åren.

5. Vilken sorts information är det som har inhämtats och i vilken form?

   Ingen uppgift kan lämnas, men man anser sig utsatt för så kallad credential harvesting (= storskalig insamling av uppgifter av kriminella nätverk som avser att sälja informationen vidare).

6. Vilka särskilda konsekvenser bedömer ni att angreppen medfört för ert företag?
   Ingen uppgift kan lämnas.

7. Hur stora kostnader kan de fullbordade angreppen antas ha medfört i affärsmässigt hänseende?
   Cirka 5 miljoner kronor/år i fullbordade fakturabedrägerier.

8. Har ni vidtagit några skyddsåtgärder med anledning av angreppen?
   Ja

9. Om ja – vilka skyddsåtgärder?
   Säkerhetsansvariga finns internt. Regelverk och rutiner på plats samt kontinuerlig utbildning av medarbetare. Sedvanliga tekniska skyddsåtgärder i form av brandväggar och spamfilter installerade. Ett så kallat EDR-system (anomalidetektering) är också installerat och servas av extern tjänst från ett svenskt företag som sköter SOC-tjänsten (security operations centre).

10. Hur stora kostnader kan skyddsåtgärderna antas ha medfört?
    Cirka 8 miljoner kronor/år.

11. Vilka bedömer ni är de mest frekventa aktörerna: konkurrentföretag/främmande makt/kriminella/anställda/annan aktör?
    Kriminella

12. Vilka angripare bedömer ni vara mest problematiska/svårast att motverka?
    Den eller de som besitter stor teknisk färdighet och har kartlagt företagets organisation. Skulle man lyckas stoppa produktionen skulle det potentiellt sett kunna vara katastrofalt. När angrepp mot företaget lyckats har det oftast skett via små kunder eller underleverantörer med bristfällig kompetens inom området it-säkerhet.

13. Har ni någon gång vidtagit rättsliga åtgärder för att motverka angrepp?
    Polisanmälan har skett i vissa fall.

14. Har dessa åtgärder lett till något resultat?
    Nej

15. Hur ser ni på den svenska statens förmåga att skydda svenska företag mot dessa angrepp och att stödja dem avseende påföljande skyddsåtgärder?
    Den är svag. MSB har någon slags funktion på området, men har ej kontaktats.

16. Hur ser ni på EU:s förmåga att skydda och stödja unionens företag i ovan avseende?
    Ingen uppfattning.

17. Vilka statliga policyförändringar skulle ni vilja se avseende bekämpning av industrispionage/cyberbrottslighet?

Finland är ett gott exempel på att staten tar ett visst ansvar också för it-säkerheten. Där finns möjligheter att spärra nätsurfande till kända kriminella sajter – man kan inte komma åt dylika hur som helst. FRA i Sverige borde få större resurser. Man har egna underhandskontakter med polisen avseende nya hot och angreppsmetoder, men det är inte tillräckligt. För övrigt borde rättsstaterna samla sig för att motverka de så kallade safe havens för cyberbrottslighet som finns för närvarande. De används av både storskaligt kriminella nätverk och av statliga angripare som av olika skäl vill maskera sin delaktighet i angrepp.

Allmän reflektion om så kallade molntjänster

Molntjänsterna har kommit för att stanna. Det tyska försöket att bygga upp en nationell molntjänst havererade, förmodligen av kostnadsskäl. Företaget kan för egen del, av produktionsrelaterade skäl, inte använda molntjänster fullt ut. Ett antal hybridlösningar kommer sannolikt att kvarstå.

Samtal med konsulter avseende SME-företag

Vad avser situationen för små och medelstora företag har Svenskt Näringsliv valt att inhämta synpunkter från erfarna säkerhetskonsulter. Utgångspunkten har varit den hotmiljö avseende industrispionage och cyberbrottslighet som möter små och medelstora svenska företag. Följande är en sammanfattning av dessa samtal.

Samtal med Richard Oehme, senior rådgivare, Knowit Cybersecurity and Law AB, tillika ordförande i Säkerhets- och försvarsföretagens (SOFF) cyberförsvarsgrupp

Företag, oavsett storlek, kan vara utsatta för industrispionage. Det som framför allt kan påverka om man är utsatt är om man på något sätt ligger i framkant av dagens teknikutveckling. Företag inom cleantech eller biomedicin är typexempel på områden där man kan tilldra sig intresse från oseriösa konkurrenter, kriminella eller statsaktörer.

Beträffande cyberbrottsligheten i allmänhet är små och medelstora företag utsatta i lika stor utsträckning som alla andra företag. Den största risken för dessa är för närvarande främst att bli utsatt för så kallade kidnappningstrojaner (ransomware), det vill säga att en kriminell aktör infekterar företagets system med skadlig programvara, krypterar densamma och sedan kräver en lösensumma för att ”låsa upp den”.

Små och medelstora företag utsätts för hela paletten av brottsverktyg, så kallad phishing via e-post eller på annat sätt infekterade dokument, verktyg eller vad helst man kan komma åt på nätet. I grunden handlar det om att den illasinnade aktören försöker komma åt personlig information av olika slag – dina inloggningsuppgifter, konto-nummer, lösenord etc. – allt i syfte att på något sätt kunna iscensätta ett bedrägeri. Som exempel nämns ett litet företag inom verkstadsindustrin som för 3–4 år sedan utsattes för just ett angrepp med ransomware. Företaget kunde på grund av att alla it-system var låsta inte producera över huvud taget. Läget var kritiskt för företaget men hotet kunde till slut avvärjas. Ett annat exempel är ett mindre företag i logistikbranschen som på grund av bristfällig it-säkerhet förlorade sin under flera år utvecklade innovation till ett annat land, i det här fallet sannolikt Kina.

Utvecklingen av dessa brottsliga angrepp kan närmast beskrivas som lavinartad och har ökat under covid-19. Problemet, särskilt för små företag, är att de oftast inte har ett bättre skydd än vilken privatperson som helst. Öppenheten mot internet är i många fall total, det vill säga i princip inga skydd över huvud taget då säkerhetsmedvetandet ofta

är lågt. I medelstora företag är medvetenheten generellt något bättre fastän det även här finns stora brister. Säkerhetskunnig personal inom företagen har ofta predikat om behovet av skyddsåtgärder för döva öron i ganska många år innan någon åtgärd har vidtagits. Behov av skydd för it-systemen har ofta fått stå tillbaka för andra prioriteringar som företagen bedömer som mer nödvändiga. Det finns dock en trend att allt fler inser att de måsta skydda sina it-miljöer enligt Oehme, vilket har lett till att allt fler har förbättrat sitt skydd under senare år.

För de flesta små- och medelstora företag skulle det räcka med att upprätthålla några grundläggande säkerhetsåtgärder för att få ett bättre skydd. Sådana åtgärder kan vara att säkerställa att säkerhetsuppdateringar (patchar) från olika produktleverantörer installeras skyndsamt. När det sedan gäller de som utkontrakterar hela eller delar av sin it-miljö brister det ofta i kompetens avseende kravställning, liksom i efterföljande kontroller av att leverantören verkligen uppfyllt sina åtaganden.

En utmaning är att mörkertalet fortfarande är stort och att alltför många när de blir drabbade av en så kallad kidnappningstrojan (ransomware) fortfarande helst vill sopa saken under mattan och gå vidare. En stor utmaning är här att rättsliga åtgärder efter en attack som denna i princip är obefintliga. Men som princip bör man dock polisanmäla denna typ av brottslighet, för att minska mörkertalet och för att tydliggöra för beslutsfattare att detta är ett problem som inte försvinner och som behöver åtgärdas.

Statens ansvar på området är delegerat mellan flera departement och statliga myndigheter. Den statliga styrningen blir därmed splittrad, och det finns ingen del av statsmakten som har en samlad syn på vare sig it-frågor i allmänhet eller it- och informationssäkerhetsfrågor i synnerhet. Utan att ifrågasätta den goda viljan kan man därför konstatera att staten för närvarande saknar det instrument som skulle erfordras för att verkligen ta ordentligt grepp om dessa frågor. Det nya cybersäkerhetscentrumet är ett steg i rätt riktning, men långt ifrån tillräckligt.

Beträffande EU:s verksamhet på området går det åt rätt håll, men med den normala trögheten som finns i EU:s processer. NIS-direktivet var ett steg i rätt riktning och nu senast införandet av den så kallade cyberakten med fokus på cybersäkerhetscertifieringar. Nu kommer också den nya cybersäkerhetsstrategin och NIS 2 som innebär nya viktiga steg.

Avslutningsvis konstaterar Oehme att Sverige, med sin höga grad av digitalisering och bredbandsutbyggnad, är extra känsligt för cyberangrepp totalt sett.

Samtal med Janne Haldesten, grundare och seniorspecialist, Sectyne AB

Små och medelstora företag är generellt sett inte utsatta för cyberspionage. Det finns dock ett antal små och medelstora företag som till exempel bedriver forskning eller sitter på information som kan vara av värde för statsstödda aktörer. Däremot kan ett angrepp mot till exempel ett mindre företag ingå som ett led i en så kallad supply chain-attack mot ett större företag. SME-företag är dock likt många andra verksamheter utsatta för ransomware och olika former av cyberbrottslighet rent generellt. Man förstår kanske i grova drag vad som kan inträffa, men skyddar sig oftast genom

slentrianköp, i bästa fall av en brandvägg och ett antivirusprogram. I de fall man blir utsatt kan det även handla om att det inte är det som finns i företagets datorer som är intressant, utan maskinen eller maskinerna i sig – utifrån åtkomst till andra system, eller för användning i ett så kallat botnet.

SME-företag har oftast ingen egen kompetens på it-säkerhetsområdet, och ofta inte heller råd att anställa sådan expertis. Ekonomin är också en mycket trång sektor, där det vanligen är ekonomiska överväganden som får avgöra huruvida man skaffar sig adekvat skydd – inte själva behovet. Många av dessa företag flyttar därför ut i det så kallade molnet, där de tjänster som erbjuds för det mesta är bättre än vad man själv skulle ha kunnat åstadkomma. Medvetenheten om riskexponering är som regel låg. När anställda är i rörelse, utanför det egna yttre skyddet och till exempel använder hotellbaserade wifi-nätverk, blir dessa mer sårbara. Även borttappade usb-minnen kan spela en roll för att kompromettera företagets skydd.

Den svenska staten har i det stora hela ingen roll i att skydda företag mot it-angrepp. De är därvidlag i samma utsatta position som kommunerna. Ansvaret för it-säkerhetsfrågor är uppdelat på några myndigheter, varav ingen har något övergripande ansvar. Det nationella centrum för it-säkerhet som ska byggas upp borde därför få en vidare roll som även inkluderar näringslivet. Det behövs mer av informationsdelning och praktisk rådgivning för att SME-företag ska kunna dra nytta av statens aktiviteter på detta område, något som i många stycken inte är helt okomplicerat. Att publicera övergripande åtgärdslistor har litet värde om mottagaren inte besitter egen förmåga att översätta de allmänna råden till handling, där olika typer av konkreta verktyg blir nödvändiga. Ett stort problem är att många företag inte har koll på grundläggande saker som vad som finns i det egna nätverket och vilka applikationer man använder, där det blir svårt att skydda det man inte vet att man har. Vidare tenderar många företag att fokusera på de senaste säkerhetshoten fastän man inte har åtgärdat äldre sårbarheter. Att då börja propagera för skyddsåtgärder på hög nivå nyttar föga. Sammantaget behövs det en starkare vilja och en avsevärt mer tydligt definierad roll för staten gentemot näringslivet.

EU:s roll på detta område har förstärkts, där EU-myndigheten Enisa har fått större ansvar och befogenheter, liksom uppkomsten av nya säkerhetsstandarder där vissa av dessa (såsom ETSI 303 645 för IoT-enheter) nu också börjar att bli nationella krav i många länder i syfte att höja den nationella informationssäkerheten. Europol och Interpol spelar en viktig roll, men generellt sett behövs det betydligt mer internationell samverkan i syfte att hålla jämna steg med en hotbild som idag är global.

Samtal med Johan Wiktorin, managing partner, INTIL Group AB

Industrispionage förekommer också mot små och medelstora förtag. Men det torde vara aktuellt främst i den mån man sitter på speciell teknologi, är underleverantör till ett större företag i försvarssektorn eller gör affärer med det femtontal länder som Säpo utpekat som problematiska.

I allmänhet är små och medelstora företag utsatta för samma risker som alla andra. I allt väsentligt utgörs cyberbrotten av försök till bedrägeri i olika former, vanligen genom betalning av falska fakturor som på ett eller annat sätt innästlats i företagets system. I ett fall hade angriparen lyckats manipulera vd:s mejlkonto för att möjliggöra ett sådant brott. Dessa bedrägerier kostar mycket pengar, både i oriktiga utbetalningar och de utrednings- och eventuella skyddsåtgärder som sedan måste vidtas. Ett särskilt utsatt område är logistiksektorn, där man ofta hanterar gods till stora värden. Där förekommer det ren infiltration av kriminella – insiders – som söker uppgifter om värdefulla transporter eller ger andra tillgång till företagets it-system, till exempel genom användning av infekterade usb-minnen. Det är Wiktorins bedömning att SME-företag generellt sett gör direkt cyberbrottsrelaterade förluster på mellan 10 000 kronor/år och 10 miljoner kronor/år. Därtill kommer kostnader för utbildning och tekniska skyddssystem, för att inte tala om eventuella renomméförluster. Man brukar som en tumregel ange att 10 procent av it-budgeten bör läggas på säkerhetsåtgärder. I vilken utsträckning det görs i småföretag är en öppen fråga. Emellertid bör man inse att det inte helt går att lita på tekniska skyddsåtgärder – det är ofta mänskliga felbedömningar som har lett till förluster.

SME-företag är när det gäller tekniska skyddsåtgärder så gott som uteslutande hänvisade till att köpa nödvändiga system från stora, ofta dominerande, marknadsaktörer. De har då ofta problem med att formulera relevanta kravspecifikationer.

Den vanligaste angriparen är utan tvekan en kriminell. Om företaget inte har mycket speciella produkter eller mycket speciella kunder förhåller det sig nästan alltid så. Rättsliga åtgärder mot cyberangrepp är dock nästan alltid verkningslösa. Problemet med att attribuera, det vill säga härleda ett visst angrepp till en viss server, viss IP-adress och viss gärningsman är näst intill oöverstigligt. Svensk polis är i och för sig ganska duktiga på området, men alldeles för fåtaliga.

Den svenska statens förmåga eller vilja att skydda företag är låg – så länge det inte rör sig om försvarsrelaterad verksamhet. Grovt räknat skulle man kunna hävda att staten distanserar sig i 99 fall av 100. Den svenska förvaltningsmodellen utgör också ett hinder. Möjligen kan den senfärdighet som Sverige som stat ådagalagt hänföras till ett – milt talat – mycket sent uppvaknande avseende betydelsen av it-säkerhet, inte bara i försvarshänseende utan för hela samhällets funktionalitet. Det nationella centrum för cybersäkerhet som nu ska inrättas är ett litet steg i rätt riktning, men anslaget är på tok för lågt. I Storbritannien läggs betydligt större belopp per capita på detta. Om Wiktorin skulle önska sig ytterligare åtgärder så vore det att staten och högskolorna i samarbete med företagen väsentligt skulle utöka volymen av relevant yrkesutbildning på cybersäkerhetsområdet – kanske tre- till femfalt, vilket också skulle skapa stora tillväxtmöjligheter av en sådan bransch. Israel är en förebild i det avseendet.

EU:s verksamhet på området har i någon mån drivit Sverige framför sig. NIS-direktivet är ett exempel på detta. Man bör också nämna EU:s cybersäkerhetsmyndighet, Enisa, som gör ett värdefullt arbete.

www.svensktnaringsliv.se
Storgatan 19, 114 82 Stockholm
Telefon 08-553 430 00

Tryck: Arkitektkopia AB, Bromma, 2021