NOVEMBER 2022

Lägesbild av Cyberhoten i Sverige

Månadens bransch: Offentlig sektor

Aktuell Hotnivå – Threatcon

Level 2: Måttlig hotnivå. Spridda attacker med övergående effekter.

1	2	3	4	5
min				max

Radar. | TRUESEC

Få rapporten varje månad: Truesec.com/monthlyreport

NOVEMBER 2022

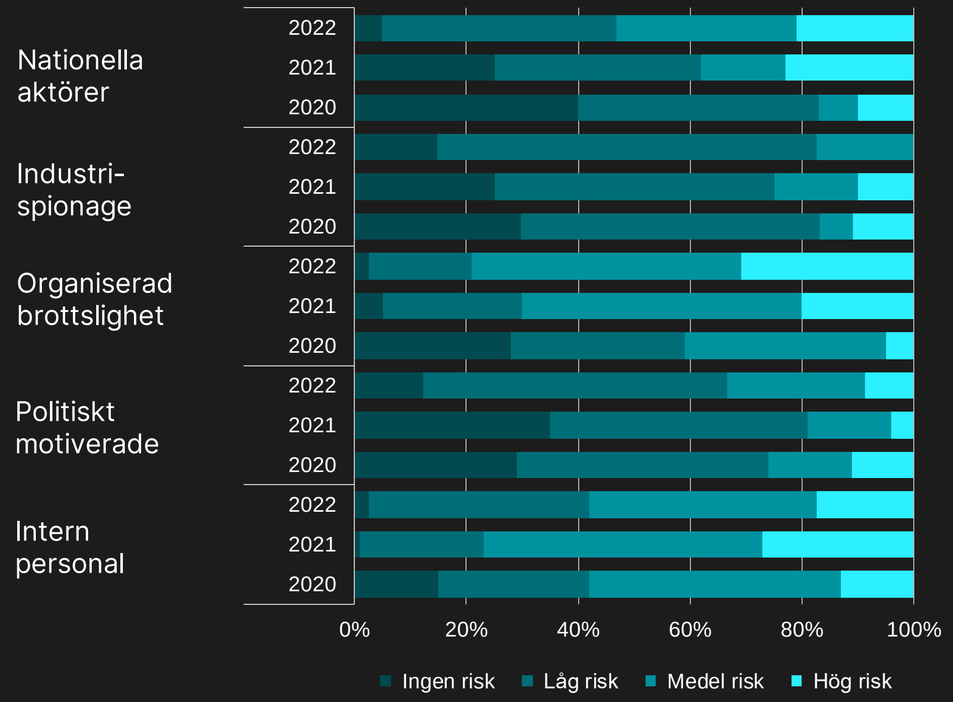
Till dig som läsare

Vi står inför en vinter, en period där det inte är ovanligt att cyberangreppen ökar till antalet. Personal som vanligtvis arbetar med förebyggande åtgärder och löpande IT-säkerhetsarbete kanske har vinterledigt, men sårbarheter upptäcks och publiceras året om. Det är en gynnsam period för angripare som får större möjligheter och mer tid på sig att genomföra IT-angrepp innan de upptäcks.

Under året har Truesec observerat hur hotgrupperingar splittras, går samman, ombildas och omformas. Initialt var mycket drivet av de kriminellas ställningstagande kring anfallskriget mot Ukraina, medan det på senare tid även påverkas av läckor och avhopp för hotaktörerna. Fortsatt är förutsättningarna för cyberbrottsligheten goda, och ingenting som kommer att försvinna i närtid. Se till att skyddet för din organisation är anpassat utifrån den hotbild som gäller för just er.

Stoppas angreppen tidigt minskar kostnad och konsekvenser kraftigt. Det är också viktigt att lära sig av de angreppen som sker, och att hela tiden förflytta IT-säkerhetsarbetet till att bli mer och mer förebyggande. Använd rätt och relevant information för detta, det finns bra information att tillgå. Det är så vi tillsammans kan få kostnaderna för att genomföra IT-angrepp ökar i relation till kostnaden för skydd.

Upplevda hot år över år, Sverige. Resultat baserat på svenska verksamheters respons på frågan “bedöm nuvarande hotbild från följande aktörer”.



Källa/data: Radar.

Upplevd hotbild

Svenska verksamheter upplever generellt en ökad hotbild inom nästan alla kategorier, förutom hot från industrispionage och den egna personal som alla backar något avseende hög och medelhög risk. Det är svårt att peka ut en enskild faktor som gör att man kan förklara den svängande trenden och orsaker till variationer i hotbedömningar, men den mediala rapporteringen av incidenter, sårbarheter och geopolitiska osäkerheter har givetvis betydande faktorer på vad som uppfattas som hot. Våra respondenters svar ligger i linje med rapporten om cybersäkerhet i Sverige.

Det man kan notera är att man inom offentlig sektor inte alls upplever hotet från organiserad brottslighet på samma sätt och särskilt som totalt mindre risk. Det omvända gäller upplevda hotbilden från politiskt motiverade aktörer och intern personal. Den förstnämnda kan tyckas självklar då vi är mycket närmare ”det officiella Sverige” inom det offentliga, men det är ändå värt att belysa denna typ av motivation och drivkraft.

Det som däremot sticker ut ordentligt är det upplevda hotet och risken från den interna personalen och våra egna medarbetare.

Lägesbild – Attacker

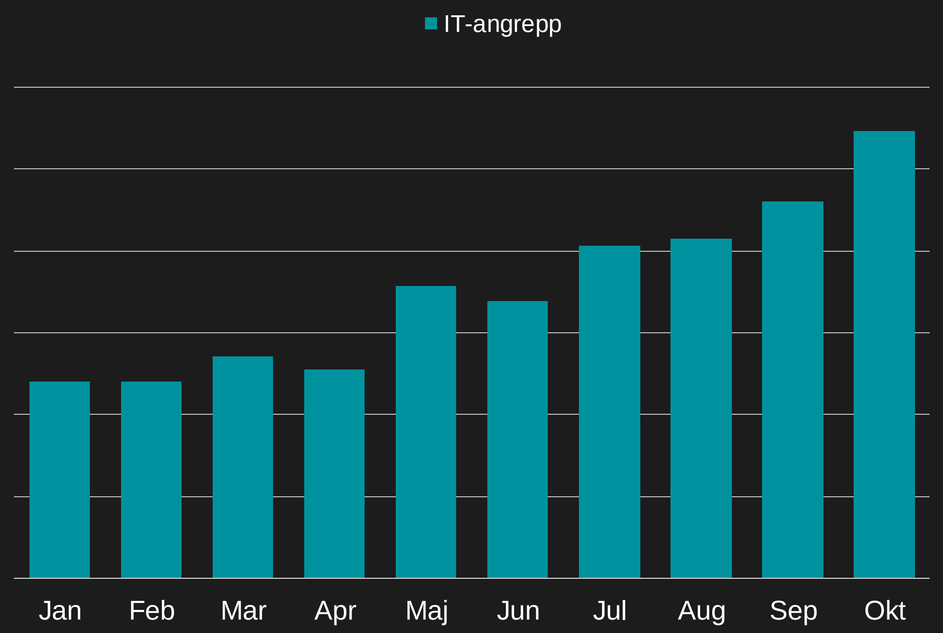
Under oktober har antalet IT-angrepp Truesec förhindrar fortsatt att öka enligt de föregående månadernas trend. Månad till månad ökade IT-angreppen med hela 19%.

Tittar vi tillbaka på tidigare år är senhösten och vintern en period där angreppen intensifieras, men det som skiljer 2022 från tidigare år är att istället för både uppgångar och dalar växlande mellan höstens månader har vi haft den här näst intill obrutna trenden av ökat antal angrepp sedan försommaren.

I ett Security Operations Center (SOC) där IT-angrepp tidigt kan desarmas ökar självklart belastningen i en sådan här trend. Men det är huvudsakligen hos organisationer som saknar kontinuerlig upptäckande och desarmerande förmåga som drabbas hårdast, där en incidenthantering behöver genomföras.

Truesec sätter tillsammans med Radar denna månad hotnivån till nivå 2, av maximalt 5. Det innebär en måttlig hotnivå där attacker till största del inte är koncentrerade, utan är spridda. Effekterna av attackerna är också mestadels övergående.

IT-angrepp, Sverige. Utveckling över tid 2022.



Källa/data: Truesec.

MÅNADENS CASE

Kapade epostkonton

En organisation drabbades av en cyberattack där en angripare lyckades ta kontroll över en e-postserver.

En av de tjänster som de flesta företag och organisationer behöver exponera är dess e-postserver. När sårbarheter dyker upp för dessa gäller det att vara snabb på att etablera extra skyddsrutiner tills dess att en uppdatering finns tillgänglig för att täppa till säkerhetshålet.

I det här fallet riktade angriparen attacken i ett tidigt skeende innan extra skyddsrutiner fanns etablerade. Målmedvetna angripare kan vänta i flera månader eller år för att en sårbarhet ska finnas tillgänglig för en viss mjukvara. Direkt eller snart efter att en sårbarhet har publiceras kan de sedan köpa sig tillgång till attackkod knuten till sårbarheten och kan fortsätta eller påbörja angrepp mot sina mål.

Källa/data: Truesec.

MÅNADENS CASE

När väl angriparen tagit sig in på e-postservern kapades snart en del epostkonton. Angriparen kunde då utnyttja identiteten hos några av de anställda för att genomföra nästa steg i angreppet, ett angrepp mot en tredje part – vilket med stor sannolikhet var det egentliga målet för angriparen.

När angriparen sedan kommit vidare med nästa steg i angreppet lämnades e-postservern, och det var när en tredje part tog kontakt och frågade om ett mejl som skickas ut som organisationen initierade incidentarbetet och händelseutvecklingen uppdagades.

Det här visa på hur stort tålamod en angripare kan ha, och hur komplext ett angrepp kan genomföras. Det visar också på att även mindre verksamhetsutövare kan bli en del i IT-angrepp där de själva inte alls är det slutgiltiga målet.

Källa/data: Truesec.

Primärt fokus och IT-budget

Svensk offentlig sektor har haft, och har, ett primärt fokus som i mycket större utsträckning än Sverige i stort har legat på innovation och transformation. Det primära fokuset på innovation och transformation ser dock en förändring nu under 2022 då man börjat röra sig mot optimering, det vill säga att vidareutveckla redan tagna investeringar. Den strategiska IT-budgeten gör gällande att detta inte bara är en läpparnas bekännelse då driftsandelen är mycket låg i jämförelse med förändringsandelen. Men även här syns nu ett genomslag genom att optimeringsdelen av IT-budgeten ökar jämfört med föregående år.

Svensk offentlig sektor, som fortsätter att investera i sin digitalisering, ökar parallellt med det sina investeringar i cyber- och informationssäkerhet samt informationsklassificering under 2022. Vidare ökar även fokuset på extern IT (IT-upphandling samt utflyttande av IT-leverans). Vilket gör det viktigt att se, tolka samt att hantera den risk som kommer genom den redan stora, och ökande, outsourcingen. Detta för att förstå hur detta kommer att påverka deras säkerhet och den risk (tredjepart) som outsourcingen innebär. Vilket kan bli problematiskt då leverantörsutvärderingar som kategori sjunker som investeringsområden för andra året i följd. Alltså bör området avseende outsourcing och utvärderingar mer eller mindre slås samman för att man ska nå någon typ av Due Dilligence med återkommande säkerhetsrevisioner hos utvalda och betrodda leverantörer.

Specifika investeringsområden. Siffra anger andel verksamheter som avser att investera i respektive specifika område, angivet i procent.

	Offentlig sektor			Sverige		
	2020	2021	2022	2020	2021	2022
Införande av AI och kognitiva lösningar	45	18	6	21	14	11
Införande av blockchainbaserade lösningar	0	0	3	1	0	2
Digitalisering av verksamhetens processer	86	82	82	60	42	61
Införande av igenkänningsteknik	3	3	3	4	2	4
Säkerhet (cyber- och informationssäkerhet)	62	68	70	48	38	74
Internet of things (IoT) och sensorteknik	28	18	21	12	13	21
IT-upphandling och avtalsrevisioner	21	24	39	23	16	25
Leverantörsutvärderingar och prisjämförelser	14	3	0	12	7	11
Kompetensförsörjningsstrategi	17	18	21	13	10	21
Omvärldsanalys och bevakning	21	13	18	16	7	14
Informationsklassificering	55	40	52	27	21	32
Insourcing eller "hemtagande" av IT-leverans	3	8	3	6	5	11
Utflyttande av IT-leverans till extern leverantör	28	16	21	13	8	26

Källa/data: Radar.

Prioriteringar hos svenska verksamheter. Siffra anger prioritering (placering där 1 är högst prioriterat) för respektive specifika område i svenska verksamheters.

	Offentlig sektor (Sverige)			
	2019	2020	2021	2022
Säkerhet (strategi & efterlevnad)	3 (4)	5 (5)	3 (2)	1 (1)
Digitalisering (förändra verksamhets- & affärsmodeller)	4 (5)	- (-)	2 (3)	2 (5)
Automatisering (nyckelprocesser)	5 (2)	- (-)	4 (1)	3 (2)
Säkerhet (teknik)	14 (14)	17 (12)	11 (11)	4 (7)
Öka automatiseringsgrad	1 (1)	2 (2)	6 (8)	5 (12)
Applikationer (förvaltning av befintliga)	9 (8)	7 (4)	8 (6)	6 (4)
Infrastruktur (införande av ny)	- (-)	12 (9)	9 (12)	7 (11)
Styrning (IT Governance)	6 (9)	6 (6)	10 (10)	8 (9)
Ökad digitaliseringsgrad	2 (3)	4 (1)	1 (4)	9 (10)
Uppfylla lagar och regler (Compliance)	12 (13)	14 (8)	13 (17)	10 (20)

Källa/data: Radar.

Prioriteringar och utmaningar

Offentlig sektor som länge haft fokus på att digitalisera (läs: effektivisera och rationalisera) sin verksamhet med IT. Detta visar sig genom att offentlig sektor i mycket större utsträckning, och under längre tid, prioriterat digitalisering och automation – vilka båda haft topp-3 prioritering under lång tid. Säkerhet (strategisk) har också legat som en topp-5 prioritering, så också säkerhet (utbildning och medvetenhet). Den sistnämnda har dock 2022 trillat ur topp-10 medan säkerhet (teknik) har hoppat upp rejält mot föregående år för att nu 2022 vara en topp-5 prioritering.

Att prioriteringarna ser ut som de gör visar att svensk offentlig sektor tagit säkerhetsfrågan på allvar, precis som Sverige i stort. Dock är det något överraskande att se att teknisk säkerhet har gjort ett så pass stort hopp avseende prioritering. En anledning till detta kan vara att man under lång tid fokuserat stort på ”mjuka delar” (strategi, utbildning, medvetenhet) parallellt med att man samtidigt påfört komplexitet genom sin digitalisering och att man nu ser att teknikområdet behöver rustas upp efter flera år i ”skymundan”.

IT-styrning samt har alltid varit prioriterad i svensk offentlig sektor, något högre än jämfört med Sverige i stort. Frågan som skall ställas är om IT-styrningen också byggts/byggs ihop med cybersäkerhet på ett sätt som skulle kunna liknas vid en Due Dilligence för att undersöka och hantera tredjepartsrisk (se föregående slide) – resultatet är något som endast tiden kan visa.

Utmaningar hos svenska verksamheter. Siffra anger utmaning (placering där 1 är störst utmaning) för respektive specifika område i svenska verksamheter.

	Energi (Sverige)			
	2019	2020	2021	2022
Digitalisering (förändra verksamhets- & affärsmodeller)	1 (5)	- (-)	1 (2)	1 (2)
Säkerhet (strategi & efterlevnad)	3 (4)	8 (3)	2 (1)	2 (1)
Kompetensförsörjning	4 (2)	3 (2)	5 (4)	3 (4)
Uppfylla lagar och regler (Compliance)	8 (14)	11 (10)	6 (7)	4 (8)
Säkerhet (teknik)	12 (12)	13 (14)	8 (5)	5 (5)
Automatisering (nyckelprocesser)	5 (3)	- (-)	15 (11)	6 (11)
Säkerhet (utbildning & efterlevnad)	- (-)	10 (6)	4 (3)	7 (3)
Ökad digitaliseringsgrad	2 (1)	2 (1)	3 (9)	8 (9)
Applikationer (förvaltning av befintliga)	10 (6)	12 (7)	10 (8)	9 (10)
Digitalisering (förstå och hantera digital affärsrisk)	- (-)	- (-)	- (-)	10 (15)

Källa/data: Radar.

Prioriteringar och utmaningar

Utmaningarna följer ganska väl prioriteringarna inom offentlig sektor. Den största utmaningen är kopplad till digitalisering, och har varit sådan i många år. Samma sak gäller för den för 2022 näst största utmaningen – strategisk säkerhet. Till skillnad från Sverige i stort ses inte strategisk säkerhet som den största utmaningen, vare sig i år eller förgående år. Vidare sjunker utbildning och medvetenhet som utmaning vilket kopplar till att prioriteringen runt området också sjunkit (till och med fallit ur topp-10). Detta kan tyckas vara anmärkningsvärt när utbildning och medvetenhet fortfarande ses som en relativt stor utmaning men samtidigt som området tappar avseende prioritering. Teknisk säkerhet ökar som utmaning och följer därigenom prioriteringen.

Kompromissen mellan säkerhet och innovation, som vi pratat om tidigare, är mindre idag då frågan får allt större uppmärksamhet i ledningsgrupperna, troligtvis tack vare rapporterade attacker i media men också uppmaningar och krav från myndigheter. Offentlig sektor som har ett samhällsuppdrag och ansvar för samhällskritisk funktioner har levt länge med regulatoriska krav vilket också syns i prioriteringarna avseende strategisk säkerhet, men också avseende att frågan om att uppfylla lagar och regler som blir allt viktigare och därigenom också en allt större utmaning – större än för Sverige i stort.

TRUESEC

Truesec är ett globalt cybersäkerhetsföretag med ett tydligt syfte: Skapa säkerhet och hållbarhet i en digital värld genom att förhindra cyberintrång och minimera påverkan. Under åren har Truesec fått ett starkt rykte och förtjänat förtroende från organisationer över hela världen. Idag består Truesec av 250+ dedikerade cyberspecialister som täcker hela spektrumet av cybersäkerhet.

– ”Det viktigaste att börja med är att investera i en bra förmåga att upptäcka dataintrång, och sen kunna göra snabba åtgärder så det inte leder till stora skador”, säger Marcus Murray.

Marcus Murray
marcus.murray@truesec.se
+46 (0)70 918 30 01

För mer information: www.truesec.com

Radar.

Radar är ett litet men starkt team av analytiker och rådgivare som tack vare lång expertis och spetskompetens är det naturliga valet gällande lokala, oberoende, datadrivna insikter för IT-ekosystemets alla aktörer.

Vi på Radar vill vara med och bidra till att svenska företag blir vinnare på omvärldsutvecklingen. Starka företag leder både till ett starkare samhälle och ett starkare Sverige. Cybersäkerhet utgör en stor utmaning och en verklig affärsrisk och handlar om så mycket mer än bara teknik.

– Säkerhetsarbete är viktigt och det har saknats svensk information som är enkel att ta till sig. Det här är nästa steg i att hjälpa IT-Sverige höja garden förstå hur hotbilden utvecklar sig öppet för alla och inga hemligheter - det vinner vi alla på.

Hans Werner
hans.werner@radargrp.com
+46 (0)73 539 15 51

För mer information: radargrp.com

Få rapporten varje månad: Truesec.com/monthlyreport