LÄGESBILD AV CYBERHOTEN I SVERIGE

AKTUELL HOTBILD OCH UTVECKLING FÖR SVERIGE.
MÅNADENS BRANSCH/EXEMPEL: SVENSK INDUSTRI

SEPTEMBER 2022

AKTUELL HOTNIVÅ – THREATCON

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

Radar. | TRUESEC

TILL DIG SOM LÄSARE

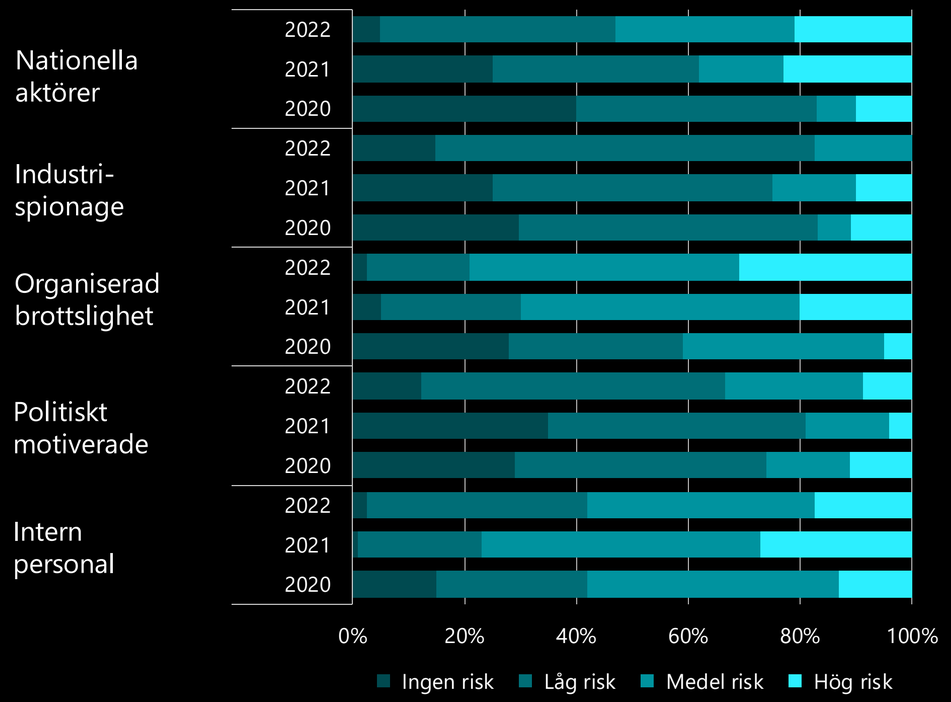
Cyberhoten mot Sverige och svenska verksamheter förändras ständigt. I ett unikt samarbete mellan Radar och Truesec vill vi ge dig som verksam i Sverige förutsättningar att arbeta datadrivet med risker kopplat till cyberhot för att kunna förebygga dataintrång.

Radar har stor mängd data och insikter rörande prioriteringar och IT-budgetar. Cybersäkerhetsbolaget Truesec har genom sin verksamhet med ett ledande incidenthanteringsteam och Security Operations Center både bred och djup insikt i nuvarande hotlandskap. Tillsammans väljer vi att presentera data och insikter i återkommande rapporter, varje gång med en fördjupning i en specifik bransch. Denna gång fördjupar vi oss inom den svenska industrin.

För att mäta nivån av cyberhotet över tid, lanserar Radar och Truesec tillsammans verktyget ThreatCon. ThreatCon anger rådande hotnivå för IT-attacker riktade mot Sverige utifrån faktiskt genomförda IT-attacker i relation till förmågan till skydd. Nya bedömningar görs löpande och presenteras på en skala mellan 1 (lugnt), 2 (normalt) upp till 5 (max).

Vi hoppas att rapporten blir användbar för dig som läsare och ser fram emot att utveckla innehållet och upplägget tillsammans för att ge Sverige tillgång till en datadriven lägesbild över cyberhotet som också är enkel att ta till sig.

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.

För tillverkande industri, som är månadens bransch i fokus, gäller ungefär samma upplevda hotbild med det stora undantaget att industrispionage upplevs utgöra en mycket högre risk. Även hot från andra nationella aktörer bedöms vara högre risk än för övriga svenska branscher.

Oron för båda dessa typer av hotaktörer kan vi koppla till upplevda risken, eller till och med affärsrisken, att bli av med skyddade affärshemligheter och IP (intellectual property) tillsammans med den upplevda sannolikheten att man nu har en måltavla på sin organisation.

LÄGESBILD – ATTACKER

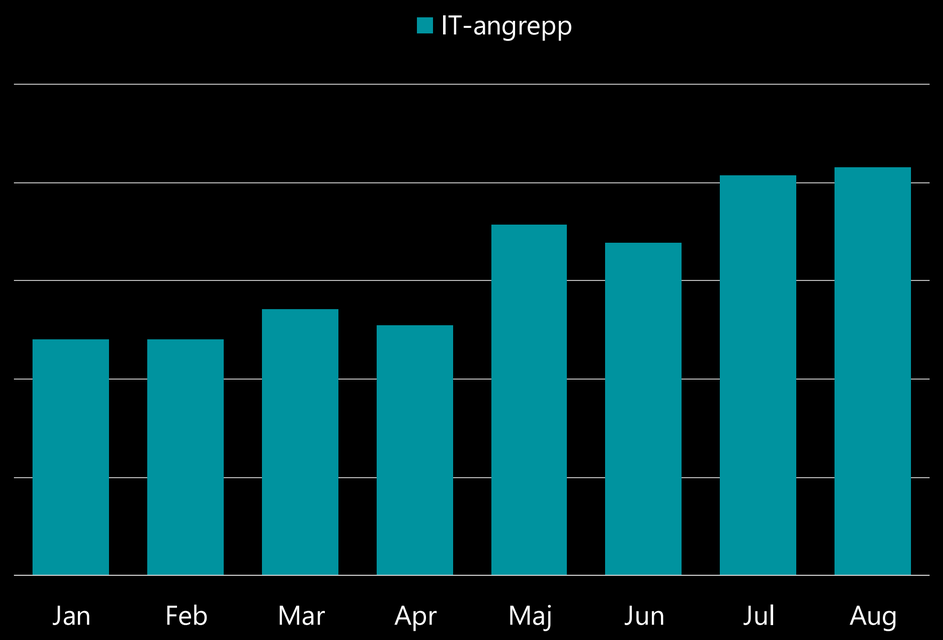
Under augusti observerar Truesec en uppgång av IT-attacker mot svenska företag på 2 procent relativt juli. En måttlig uppgång, men i det stora perspektivet innebär det en fortsättning på den stigande trend av IT-attacker som påbörjades i maj.

Efter en vinter och tidig vår med färre IT-attacker än normalt tog det en rejäl vändning under maj med en ökning på 40 procent. Därifrån har Truesec sett en markant uppgång av IT-attacker mot svenska företag. Ökningen sedan april är på 63 procent och slår brett över flera branscher.

Underlaget baseras på berikat data där analytiker i varje enskilt fall gjort bedömningen att det rör sig om en IT-attack som om det inte stoppats kunnat leda till allvarliga konsekvenser för det drabbade företaget. Se månadens exempel för en tänkbar utveckling om sådana incidenter inte detekteras och avväpnas skyndsamt.

Baserat på presenterat och bakomliggande data om hotbild och omvärld väljer Truesec tillsammans med Radar att ange hotnivån till nivå 2, av maximalt 5. Detta 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: SVENSK INDUSTRI

BRISTANDE UPPDATERINGAR LEDDE TILL UTPRESSNINGSATTACK

Under våren 2022 fick Truesec i uppdrag att hantera ett allvarligt ransomware-angrepp på ett skandinaviskt företag. Det visade sig att angreppet hade skett i två steg. I det första steget som inträffade redan under vintern, hade en hotaktör utnyttjat en känd sårbarhet i Microsoft Exchange för att erhålla tillgång till nätverket. Trots att denna sårbarhet var publicerad och publikt tillgänglig i flera månader hade företaget aldrig applicerat säkerhetsuppdateringen.

När denna hotaktör fått tillgång till nätverket installerades en så kallad cryptominer, en skadlig kod som stjäl datorkraft för att producera kryptovaluta. Denna hotaktör var sannolikt i första hand intresserad av att sälja accessen till andra cyberbrottslingar. Den skadliga koden var ett sätt att tjäna lite extra pengar i väntan på försäljning.

Källa/data: Truesec.

MÅNADENS CASE: SVENSK INDUSTRI

Efter två månader tyder mycket på att det har skett en transaktion på DarkWeb, där den hotaktör som först fått fotfäste på företagets nätverk nu sålt den åtkomsten till en annan hotaktör. Den nya hotaktören gick då in och stängde ned cryptominern och började ta kontroll över hela nätverket och kryptera all information. Ett fullskaligt ransomware-angrepp var ett faktum och hotaktören försökte pressa företaget att betala kryptovaluta för att få tillbaka den krypterade informationen.

Detta visar att breda mass-angrepp där sårbarheter i mjukvaror utnyttjas för att erhålla fotfäste i mängder av sårbara system, kan leda till mycket svåra angrepp flera månader efter att en hotaktör först lyckats få fotfäste. Det visar också att all skadlig kod som körs i gång inne på ett nätverk är allvarliga, även om den i sig inte har kapacitet att åstadkomma svår skada, så kan hotaktören tjäna stora pengar på att sälja åtkomsten till andra brottslingar med syften där konsekvenserna blir mycket allvarligare.

Källa/data: Truesec.

PRIMÄRT FOKUS OCH IT-BUDGET

Industrin som generellt reagerar snabbare än det nationella genomsnittet på bland annat konjunkturförändringar har återigen börjat skifta sitt fokus mot kostnadsreduktion. Vidare är det värt att nämna att industrin i större utsträckning också haft en försiktigare optimeringsstrategi bortsett från 2020 då man i större utsträckning än det nationella genomsnittet satsade på innovation genom IT.

Historiskt sett har stort fokus på innovation ofta inneburit en lägre prioritet avseende säkerhet. Våra prioriteringar har lett till att olika investeringsområden har förändrats över tid, vilket också lett till skillnader i specifika investeringsområden mellan industrin och det nationella genomsnittet.

Industrin ökade sina investeringar i säkerhet kraftigt redan 2021 samt att digitalisering backat tillbaka till nivåerna som de såg ut 2020. Vidare och intressant att notera är att IoT är ett område som ökar medan informationsklassificering backar. Detta antyder att flertalet redan är på det klara med vilken information som ska gå genom noderna eller så är det ett område som kan komma med betydande utmaningar i ett senare skede. Båda grupperna ökar sin outsourcing vilket också kan komma med utmaningar i framtiden om man inte är på det klara med hur information kommer utsättas för risk i långa och komplexa kedjor.

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

	Industri			Sverige		
	2020	2021	2022	2020	2021	2022
Införande av AI och kognitiva lösningar	8	0	9	21	14	11
Införande av blockchainbaserade lösningar	4	0	0	1	0	2
Digitalisering av verksamhetens processer	69	78	68	60	42	61
Införande av igenkänningsteknik	8	0	0	4	2	4
Säkerhet (cyber- och informationssäkerhet)	46	67	64	48	38	74
Internet of things (IoT) och sensorteknik	15	22	27	12	13	21
IT-upphandling och avtalsrevisioner	27	0	14	23	16	25
Leverantörsutvärderingar och prisjämförelser	15	0	18	12	7	11
Kompetensförsörjningsstrategi	8	11	14	13	10	21
Omvärldsanalys och bevakning	19	0	9	16	7	14
Informationsklassificering	23	22	9	27	21	32
Insourcing eller "hemtagande" av IT-leverans	8	0	14	6	5	11
Utflyttande av IT-leverans till extern leverantör	12	33	32	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.

	Industri (Sverige)			
	2019	2020	2021	2022
Säkerhet (strategi & efterlevnad)	5 (4)	7 (5)	1 (2)	1 (1)
Automatisering (nyckelprocesser)	1 (2)	- (-)	1 (1)	2 (2)
Säkerhet (utbildning & medvetenhet)	- (-)	11 (10)	6 (7)	3 (3)
Applikationer (förvaltning av befintliga)	8 (8)	2 (4)	13 (6)	4 (4)
Applikationer (införande av nya)	- (-)	5 (3)	2 (5)	5 (6)
Infrastruktur (förvaltning av befintlig)	6 (7)	6 (13)	7 (9)	6 (8)
Säkerhet (teknik)	10 (14)	10 (12)	12 (11)	7 (7)
Ökad digitaliseringsgrad	3 (3)	1 (1)	3 (4)	8 (10)
Digitalisering (förändra verksamhets- & affärsmodeller)	7 (5)	- (-)	8 (3)	9 (5)
Styrning (IT-organisation)	11 (9)	3 (6)	13 (10)	10 (9)

Källa/data: Radar.

PRIORITERINGAR OCH UTMANINGAR

Prioriteringar och utmaningar skiftar år för år men vi har alltid haft en tonvikt på förändring. Under pandemiåret (2020) bubblade kostnadsreduktion tillfälligt upp genom att kvala in i topp-10 (dock ej för industrin) som i övrigt såg införande av nya applikationer, digitalisering och automation högt prioriterade områden. Säkerhet som alltid setts som ett prioriterat område (och en utmaning) i svenska organisationer fick dock lägre prioritet under pandemiåret 2020. Under 2021 återgick prioriteringarna till att likna läget innan pandemin, det vill säga ett större fokus på digitalisering och automation men också säkerhet.

Som ett av de mest digitaliserade länderna inom EU har Sverige historiskt sett fått se att arbetet med säkerhet fått stå tillbaka till förmån för innovation och transformation. Under 2022 blev dock säkerhet (strategisk) för första gången högsta prioritet i de flesta svenska organisationer, till och med viktigare än digitalisering och automatisering. Kompromissen mellan säkerhet och innovation är idag mindre då frågan får allt större uppmärksamhet i ledningsgrupperna, troligtvis tack vare rapporterade attacker i media men också uppmaningar och krav från myndigheter.

Precis som för det nationella genomsnittet har industrins prioriteringar varit snarlika avseende automation och digitalisering men med skillnaden att säkerhet blev högsta prioritet, före automation, redan 2021. Området halkade också ner, precis som för det nationella genomsnittet, under första pandemiåret (2020). Vilket kan resulterat i ett tapp som nu måste tas igen.

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

	Industri (Sverige)			
	2019	2020	2021	2022
Säkerhet (strategi & efterlevnad)	4 (4)	4 (3)	3 (1)	1 (1)
Säkerhet (teknik)	9 (12)	13 (14)	5 (5)	2 (5)
Säkerhet (utbildning & efterlevnad)	- (-)	5 (6)	1 (3)	3 (3)
Kompetensförsörjning	6 (2)	3 (2)	15 (4)	4 (4)
Digitalisering (förändra verksamhets- & affärsmodeller)	8 (5)	- (-)	6 (2)	5 (2)
Digitalisering (förstå & hantera digital affärsrisk)	- (-)	- (-)	- (-)	6 (7)
Öka digitaliseringsgrad	1 (1)	1 (1)	7 (9)	7 (9)
Applikationer (införande av nya)	- (-)	8 (4)	12 (6)	8 (6)
Automatisering (nyckelprocesser)	2 (3)	- (-)	4 (11)	9 (11)
Stärka verksamhetens konkurrenskraft	7 (8)	2 (8)	14 (17)	10 (14)

Källa/data: Radar.

PRIORITERINGAR OCH UTMANINGAR

Ser man till utmaningar kan man se att säkerhet legat inom topp-5 redan innan pandemin tillsammans med digitalisering och kompetensförsörjning. Teknisk säkerhet har leget som topp-5 utmaningar de två senaste åren. Detta antyder att utvecklingen runt digitaliseringen och dess möjligheter nu börjar skapa reella bryderier avseende hur man ska skydda sig.

Industrins utmaningar är snarlika det nationella genomsnittet men med skillnaden att samtliga säkerhetskategorierna (strategi, teknik, utbildning & medvetande) ligger inom topp-3, före digitalisering och kompetensförsörjning. Sett till det faktum att industrin i större utsträckning än tidigare outsourcar samtidigt som man investerar i IoT (också kallat IIoT) förstår man också att teknisk säkerhet blir en allt större utmaning. Trots att förvaltning av befintliga applikationer länge varit ett prioriterat område (bortsett från 2021) har det i exemplet som gavs i början inte alltid varit tillräckligt för att skydda organisationen mot intrång. En del i förklaringen kan ligga i att området inom industrin inte setts som en utmaning. En väl utvecklad förvaltning med säkerhet på agendan är idag ett måste, och underskattningen runt detta faktum måste brytas.

Det också intressant att notera att kompetensförsörjning som ses som en stor utmaning *inte* är ett prioriterat område. Den ständigt växande omfattningen av cybersäkerhetsaktiviteter som: sårbarhetshantering, övervakning, utbildning & medvetenhet, med mera gör att många verksamheter riskerar att hamna efter avseende sina mål innan de ens kommit i gång. En förklaring till otillräckliga satsningar ligger i kompetensbristen då två tredjedelar av svenska IT-beslutsfattare uppger att det råder brist på säkerhetskompetens. Med andra ord borde kompetensförsörjning lyftas till ett prioriterat område om man ser till utmaningarna.

TRUESEC

Truesec är ett ledande cybersäkerhetsbolag med ett tydligt syfte: Att förhindra dataintrång och minimera skadan om de inträffar. Gruppen består av över 250 medarbetare med bred expertis inom cybersäkerhet och har sedan starten 2005 levererat säkerhetslösningar till kunder inom privat och offentlig sektor, både i Sverige och internationellt.

Förmågan att övervaka, upptäcka och svara på attacker är viktiga hörnstenar i ett modernt cyberförsvar. Läs mer om Managed Detection and Response.

– ”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.

För mer information: truesec.com

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

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.

För mer information: radargrp.com

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