MAJ 2025

## CYBERSÄKERHET
## HOT, TRENDER, INCIDENTER, NYHETER

# RAPPORT

PHATHACKZ.SE

**Fatmir Neziraj**
1T-SÄK3RHET5K0NSULT

# FÖRORD

Detta är en rapport som handlar om cybersäkerhet. I första utgåvan finns det information som involverar många olika områden för att få en större bild av branschen, trender och hot. Informationen är samlad och hänvisad till respektive källor. Exempel på källor är stora internationella företag och internationella samt nationella organisationer som gör årliga, kvartalsvis, månatliga eller veckoanalyser inom cyberhot och branschen.

Mitt mål med denna rapport är att sammanställa informationen, göra den lättillgänglig och på svenska för att du som läsare ska få en enklare uppfattning och uppdatering av vad som händer inom cybersäkerhetsvärlden.

För att behålla en äkta känsla i läsningen och för att undvika uppsvällda sociala medieflöden med Ai har jag valt att, bara om nödvändigt, vid väldigt liten omfattning använda Ai eller i många fall inte alls vid skriften av denna rapport. Om användning av Ai sker så är det för idéer och bollplank vid vissa rubriker eller utformanden på hur jag ska skriva denna rapport och **aldrig** låta Ai skriva rapporten.

Ai är hett på tapeten och många avsnitt kan komma att innehålla information om Ai - även fast det är ett otroligt bra verktyg så vill jag hålla det genuint och inte låta Ai göra jobbet.

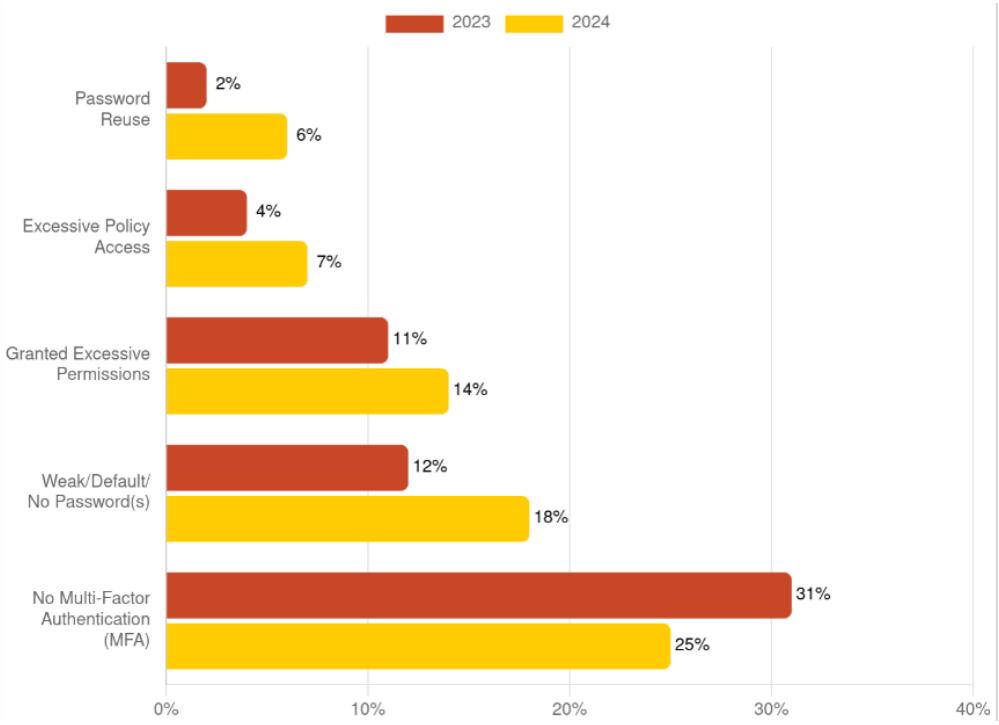
I förhand ber jag om ursäkt för stavfel och misstag i texten - detta arbete sker på min privata tid och det finns en tydlig strävan att bli bättre, feedback mottages.
För information eller kontakt med mig som skribent hänvisar jag till www.phathackz.se

# X01_

# VAD SÄGER BRANSCHEN?

Att hotet ökat är knappt någon nyhet. Omvärlden bär på oroligheter och det är inte något jag nödvändigtvis vill gå in på eftersom det inte fyller syftet för denna rapport men samtidigt ger det en tydlig förklaring på att det råder osäkerhet i vår omgivning och med det kommer aggressiva stater och grupper att trappa upp sin offensiva påverkan i cybersäkerhetsvärlden.

Något som konstant växer är "identitetsbaserade"-attacker enligt en årsrapport från Crowdstrike. Det innebär försök och attacker mot människor genom vishing, social engineering eller exempelvis köp av stulna uppgifter. Att sikta in sig på användare har visat sig vara en lyckad strategi för att ta sig in i företagens system. Det finns konton med alldeles för höga behörigheter, användarkonton för användare som inte längre jobbar, användare som återanvänder gamla lösenord eller lösenordpolicys som har för låga krav.




*Tabell från Unit42 Palo Alto Network*

Figure 2: Trends in identity and access management issues from 2023 to 2024.

I en rapport från Cisa.gov (Maj 2025) nämns det att Ryssland använder olika typer av phishingmetoder i kombination med mjukvarusårbarheter, chansning av credentials, bruteforce och utnyttjar tredjepartsrelationer med företag och olika samhällstjänster.

Rapporten visar att *en* typ av mitigation är hanteringen av identiteter, alltså Identity and Access Management. Med bättre IAM (identity and access management) kan man bättre hålla koll på konton och behörigheter med hjälp av policys och auditing. Man får också utökat stöd i form av MFA, Smartkeys, FIDO2-nycklar m.m. eftersom dessa metoder inte går att knäcka med hjälp av bruteforcing idag. Det finns även fler tekniska metoder som SSO, tillåta x antal login och separera privilegade konton från vanliga användare.

Enligt Microsoft så är mer än 99% av identitetsbaserade attacker lösenordsattacker. Microsoft har blockat 7000 lösenordsattacker per sekund, enligt rapport från 2024. Rapporten från Crowdstrike visar även den att IAM-lösningar och IAM-"hygien" är en stark mitigerande faktor.

Ett annat område som verkligen lyfte mina ögon var utnyttjande av tredjepartare.
I rapporter från Deloitte, Verizon och Crowdstrike ser man kraftiga ökningar på dessa typer av attacker.
Tredjepartsattacker innebär köp av stulna uppgifter från tidigare läckor, ransomware eller andra attacker. En annan typ av tredjeparts-påverkan som Cisa förklarar i sin rapport nämner de att Ryssland använder "relation trust", vilket innebär att de utnyttjar andra företag eller tjänster som är kopplade till slutmålet.

Låt oss säga att PhatHackz AB är företaget vi vill komma åt men vi vill inte eller kan inte göra en direkt attack mot dem. Istället letar vi efter andra kopplingar till företaget som t.ex. leveransföretag av produkter, elektriker, städtjänst eller annan typ av mjukvara som vi vet företaget använder och som skulle kunna ha sårbarheter i sin mjukvara.

Detta är även något som Säkerhetspolisen i Sverige nämner, "Säkerhetshotande verksamhet från främmande makt", i en artikel. Hotet från Ryssland, Kina och Iran är stort och dessa främmande makter använder olika metoder, bland annat tredjepartspåverkan, utnyttjande av agenter, spionage m.m. för att få information.
Verizon nämner i sin 2025 rapport att 30% av intrången sker via tredjepartsinvolvering, alltså dubbelt så stor ökning från förgående år.

# ÖKNING PÅ MÅNGA HÅLL

Det finns en tydlig ökning av dom flesta typer av cyberattacker och det kommer kanske inte som en överraskning.

Men det är inte bara mängden av attacker som ökar, det är också effektiviteten.
Med hjälp av Ai har nu cyberkriminella blivit mycket snabbare och vassare på att utnyttja sårbarheter. Det innebär att dom kan göra fler attacker samtidigt men också snabbare mot varje mål. En rapport av Unit42 (Palo alto) nämner de att en av fem intrång och läckor sker under en timmes tid. Här ser man tydlig hjälp av Ai och automatiseringar.

Under 2024 såg Crowdstrike att tiden för att förflytta sig lateralt i ett system (breakout time) var på rekordlåga nivåer. I snitt hamnade det på 48 minuter men som allra snabbast kunde det mätas på 51 sekunder. Det är alltså otroligt snabb förflyttning.

Ransomware fortsätter vara på topp enligt en rapport from Deloitte. De förklarar att RaaS-modellen (Ransomware as a service) gör det enkelt för nya grupper att etablera sig och kunde se över 30 nya grupper under 2024. Många av dessa grupper har ett finansiellt syfte eller politisk agenda bakom angreppen. Under 2024 hade gruppen "RansomHub" angripit över 500 offer i olika branschsektorer. Min egna tanke är att det är otroligt många företag men samtidigt misstänker jag att vissa av de påverkade kan vara via supply-chain attacker där liknande attack skedde mot Coop under 2021.
Deloitte ser en ökning på 17% under 2024 mot förgående år.
Microsoft ser stor ökning av Ransomware men att “slutsteget”, alltså steget där angripare krypterar datan har minskat. Det har alltså inte varit lika framgångsrikt att uppnå slutmålet.

Jag ser också ett samband mellan RaaS och så kallade third-party compromises som tidigare nämnt. Köp av stulna uppgifter och data har ökat och påverkan från tredjepart ökar i samband med detta.

I flertalet rapporter visar trenden på Malware-användning i form av "infostealers" som var virus som stal uppgifter i olika former. Det kan innebära data i dokument, lösenord, webbläsare eller annat. Enligt Checkpoint ser man en ökning på 58% sedan förgående år.

Sabotage och DDOS-attacker har också stark ökning där "state-sponsored" hackers vill påverka samhällsviktiga tjänster, tex attacker i Sverige mot banker, Swish, BankID och andra företag och tjänster i samhället. Cloudflare nämner i en rapport att antalet överbelastningattacker (DDOS) i första kvartalet 2025 hade redan **större volym** än hela året 2024.
Här ser vi stor påverkan från tidigare nämnda länder som Ryssland, Kina och Iran.

# VILKA ÄR HOTAKTÖRERNA?

I flertalet hotrapporter (Cisa, Crowdstrike, Deloitte, Microsoft, Verizon, FBI, Säkerhetspolisen) så ser vi att ett stort cyberhot kommer från Ryssland. Det är statliga aktörer eller politiskt drivna aktörer som är i toppen av attacker. Vi ser också länder som Kina och Iran samt i vissa fall Nordkorea som också finns i toppen på länder som driver offensiv cyberpåverkan i världen och i Sverige.

Om alla grupper har statlig koppling kan jag inte bekräfta men eftersom det finns politiska anledningar bakom vissa attacker så är sannolikheten hög.

Vissa av hoten kan komma inifrån, är en uppmärkning från Säpo. De visar att ryska och kinesiska säkerhets och underrättelsetjänster har starkt fokus på politiska, militära och ekonomiska mål i Sverige. Där skiljer sig Iran, som fokuserar på oppositionella diasporan, alltså enskilda individer som kanske har en högt uppsatt roll i verksamheter eller myndigheter och besitter information eller tillgång till känslig information.

# MINSKA PÅVERKAN

En trend i marknaden som ökar är området IAM - då menar jag konceptet och inte enstaka produkter. En bra hygien är A och O när det kommer till att minska påverkan av cyberattacker. För vi alla vet att det handlar om NÄR attacken sker, inte OM.

**Identity and Access Management** rankas högt upp på samtliga rapporter. Det kan i vissa fall innebära enkla åtgärder som MFA, starka lösenordspolicys, least-privilege metoder eller regelbunden granskning av användarkonton, behörigheter och lösenord.
Aktiva användarkonton (T1078 Mitre) har 41% större användning i jämfört med övriga metoder enligt Unit42 Palo Alto Networks (se nedan figur)

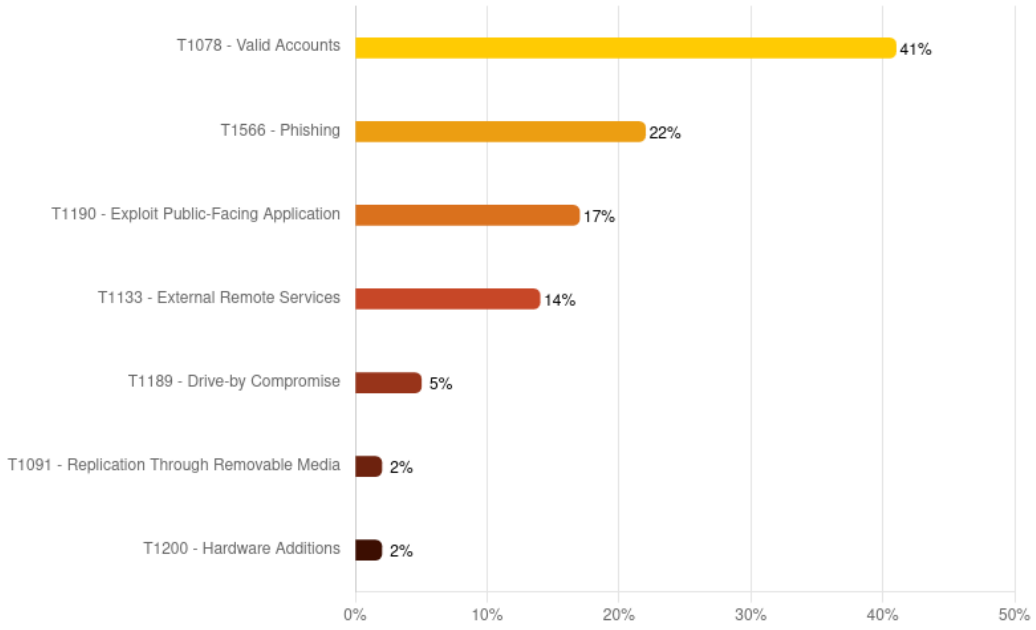



**Figure 5:** Relative Prevalence of Techniques Observed in Association With the Initial Access Tactic

Även arbetsmarknaden ser stor efterfrågan inom området IAM med fokus på stora företag och organisationer som har många användare att hantera.

**Data Protection** är också en god faktor för att minska negativa påverkan. I detta området innebär det krypteringar åt alla håll och kanter. Det innebär också att arbeta med DLP (Data Loss Protection), backuper i former på olika medier, olika platser, cloud och onprem. Kontinuerlig testning och återinläsning av data för att alltid ha relevant och fungerande data. Väldigt viktigt mot ransomware.

**Monitoring and incident response,** givetvis vill vi ha bra övervakning (SOC) av system och nättrafik för att kunna röja undan hot och snabbt vidta åtgärder. Det gäller att ha bra kontinuitetsplaner som ofta uppföljs och kontrolleras. Här innebär det också att övervaka användarbeteenden - hur reagerar användare vid filnedladdning eller phishing?

**Utbildning av användare,** ett område som jag brinner för och ofta trycker på. Det är otroligt viktigt att användare hela tiden får information och är med i utvecklingen. Finns det kända sårbarheter i mjukvara så måste informationen komma ut. Samtidigt finns det andra problem och tyvärr räcker inte endast denna åtgärd. Eftersom att mängden attacker ökar och antalet vägar in har blivit större så finns fortfarande behovet av starka tekniska skydd. Men ett starkt tänk av personal som kan identifiera social engineering eller phishing gör stora positiv påverkan.

Det finns givetvis mycket mer man kan göra för att minska påverkan av hackerattacker men denna rapport är inte rätt rapport för det. Här skriver jag istället vad som sker i marknaden, vilka behov det finns, vilka typer av attacker och trender.

# ANALYS

Vi ser en fortsatt stor ökning och 2025 lär slå förgående år i många domäner vad gäller cyberattacker. Det har till viss del redan skett.

Mycket pekar på att social engineering och Ai kommer ha fortsatt tillväxt och går ofta att kombinera till avancerande angrepp. Extra oroande är användning av Ai där utvecklare och IT-tekniker förlitar sig på kod och information som spottas ut från chatbottar.

Även fast malware har ökat i användning generellt så ser Crowdstrike att 79% av *upptäckterna* var "malware-free", alltså att man använde tekniker och metoder som inte innebar skadlig kod. De pekar på att det är en ökande trend sedan 2019 där 2023 och 2024 har legat över 75% medan under 2019 var det på 40%. Däremot verkar det saktat ner senaste 2 åren och kanske inte får lika hög ökning kommande år. Det återstår att se.
Men en anledning är att man istället utnyttjar stulna eller köpa autentiseringsuppgifter.

Från flera rapporter ökar hotet globalt och i alla marknader.
Branscher som påverkas är Tech-bolag som står för 23%, till följ av konsultbolag som står för 15% och tillverkning/industri står för 12%, enligt Crowdstrike. Microsoft pekar på IT 24%, Education and Research 21% och Government 12%. I kombination med ransomware och supply-chain attacker så kommer hoten fortsätta öka. Övriga oroligheter i omvärlden kommer också vara en bidragande faktor.

Ransomware förblir och kommer att fortsätta öka, särskilt med RaaS. Däremot ökar också åtgärder från företagen. Bättre kryptering och metoder för att motverka fullständig kryptering från angripare vid attacker.

Som tidigare nämnt så skedde förflyttningar lateralt otroligt snabbt. Här ser vi ökning inom område som måste stärkas för att minska skadan. Återigen är det Identitets och behörighetsåtkomster, förbättrad och snabbare hotidentifiering (SOC) och proaktiv omvärldsbevakning och hotanalys som kommer vara till stor hjälp.

# > C0NN3CT10N CL053D_

Tack för att du läst denna rapport. En viktig påminnelse att detta är ett projekt som sker på min fritid där jag sätter upp mina egna regler (inga regler) på hur rapporten ska se ut.

Jag vill att det ska vara kostnadsfritt att läsa på om branschen och hålla borta appar, konton och prenumerationer från gratis information.

// Fatmir
=== END OF FILE ===