dizparc

Threat Intel Report 2026

Cyberhot mot svenska SME:
Lärdomar, mönster och prioriteringar.

www.dizparc.se/cybersakerhet

Innehåll

Kapitel 1

Rapporten i korthet

Förord

Under de senaste åren har cybersäkerhet gått från att vara en teknisk specialfråga till att bli en central del av verksamheters riskbild. Samtidigt har förståelsen för vad hotet faktiskt innebär inte utvecklats i samma takt.

Mycket av det offentliga samtalet om cyberhot präglas av en bild av avancerade angrepp, sofistikerade verktyg och riktade attacker mot stora organisationer. Den bilden är inte fel – men den är ofullständig. För de flesta svenska företag ser verkligheten annorlunda ut.

De angrepp som orsakar verklig skada i svenska organisationer är sällan de mest avancerade. För små och medelstora företag handlar hotbilden i första hand om organiserad cyberbrottslighet, där angrepp genomförs systematiskt och i stor skala. Det innebär att samma typer av svagheter utnyttjas om och om igen.

Samtidigt har beroendet av digitala system, externa tjänster och leverantörer ökat kraftigt. Verksamheter är idag en del av större digitala ekosystem där gränsen mellan egen och extern risk blir allt mindre tydlig. Det förändrar inte bara hotbilden, utan också ansvaret.

Den här rapporten är skriven utifrån ett enkelt konstaterande: för att kunna prioritera rätt åtgärder behöver man förstå hur hoten faktiskt tar sig uttryck i praktiken. Inte i teorin, utan i den vardag där incidenter uppstår, hanteras och får konsekvenser.

Dizparc, April 2026

Syfte

Vår Threat Intel Report sammanställer erfarenheter från operativt cybersäkerhetsarbete under 2025 och kompletterar dessa med internationell branschdata. Data för rapporten bygger på verkliga incidenter och angrepp observerade av vårt Security Operations Center (SOC) och vårt Incident Response Team, vilket ger ett perspektiv förankrat i hur hot faktiskt tar sig uttryck i svenska organisationer.

Rapporten riktar sig primärt till beslutsfattare, IT-ansvariga och säkerhetsfunktioner, men kan även läsas av den som vill fördjupa sin förståelse för hur hotaktörer agerade mot svenska små och medelstora företag under 2025.

Syftet är att ge ett underlag för bättre prioriteringar. Genom att beskriva hur angrepp faktiskt genomförs, vilka mönster som återkommer och varför incidenter får konsekvenser, vill vi bidra till en mer verklighetsnära bild av cyberrisk. Rapporten ska inte läsas som en teknisk genomgång av enskilda hot, utan som ett stöd för att förstå helheten.

Den kan användas för att sätta riktning i säkerhetsarbetet, identifiera relevanta riskområden och skapa en gemensam förståelse mellan IT, verksamhet och ledning.

Executive **Summary**

Denna rapport bygger på operativ erfarenhet från incidenthantering, övervakning och säkerhetsanalys i svenska organisationer under 2025, kompletterat med internationell branschdata. Den samlade bilden visar ett hotlandskap som inte nödvändigtvis är nytt, men som har blivit mer systematiskt, snabbare och mer affärskritiskt i sina konsekvenser.

För svenska små och medelstora företag domineras hotbilden av organiserad cyberbrottslighet. Angrepp genomförs i skalbara modeller där angripare systematiskt söker efter svagheter i identitetshantering, exponering mot internet och kända sårbarheter. Det innebär att angrepp i hög grad drivs av sannolikheten att lyckas, snarare än av specifikt utvalda mål.

Den vanligaste angreppsvägen är fortsatt initial åtkomst via phishing och komprometterade identiteter. Under 2025 har dessa angrepp utvecklats till mer sofistikerade och flerledade processer, där komprometterade konton används för att angripa nya mål och där tidslinjen från första klick till vidare angrepp ofta mäts i minuter. Parallellt ser vi hur AI används för att öka kvaliteten och träffsäkerheten i phishing, vilket ytterligare förstärker dessa mönster.

Samtidigt ser vi ett tydligt skifte i hur snabbt sårbarheter går från att bli kända till att utnyttjas i praktiken. Fönstret mellan publicerad uppdatering och aktiv exploatering har i många fall krympt till dagar. Traditionella patchcykler, som tidigare varit tillräckliga, håller inte längre. Många organisationer arbetar fortfarande utifrån scheman där kritiska system uppdateras med veckors fördröjning, vilket skapar ett växande gap mellan känd risk och faktisk exponering.

Detta innebär ett strukturellt skifte för IT-organisationer. Att hantera sårbarheter har gått från en planerad underhållsaktivitet till en tidskritisk riskhanteringsfråga.

För många verksamheter är detta en förändring som ännu inte fullt ut har omsatts i arbetssätt eller prioriteringar.

Samtidigt visar både SOC-data och red team-övningar att det som avgör utfallet sällan är en enskild teknisk kontroll. Brister i struktur, otydligt ägarskap och avsaknad av systematiskt säkerhetsarbete är återkommande orsaker till att angrepp lyckas. Organisationer saknar ofta insyn i sina egna miljöer, vilket leder till att intrång kan pågå under lång tid utan att upptäckas.

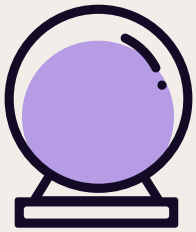
En central observation är gapet mellan upplevd och faktisk säkerhet. Många organisationer utgår från att etablerade skyddsåtgärder ger ett tillräckligt skydd, men saknar förmåga att verifiera detta i praktiken.

Hotbilden är dessutom bredare än den egna organisationen. Leverantörer, partners och externa tjänster utgör en integrerad del av den digitala miljön, och angrepp riktas i allt högre grad mot dessa relationer.

Även om hotbilden utvecklas snabbt i tempo och metodik är de underliggande angreppsmönstren ofta återkommande. Det innebär att angrepp i hög grad är förutsägbara – och därmed möjliga att förebygga och upptäcka för organisationer som arbetar strukturerat och med rätt prioriteringar.

Sammantaget pekar rapporten på ett behov av ett mer strategiskt angreppssätt. Cybersäkerhet behöver hanteras som en del av verksamhetens övergripande riskstyrning, med tydligt ansvar på ledningsnivå.

I rapportens avslutande kapitel sammanfattas de åtgärder som vi ser har störst effekt i praktiken, med fokus på att skapa insyn, korta ledtider i hantering av sårbarheter och etablera ett mer systematiskt och ägarskapsdrivet säkerhetsarbete.



Kapitel 2

Det större perspektivet

Hotlandskapet 2026: En omvärld i förändring

Huvudskribent

Christoffer Widjeback, Cybersäkerhetsexpert, Dizparc Karlstad

Ett förändrat säkerhetsläge och ett mer strukturerat cyberhot

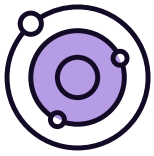
Det svenska cyberhotlandskapet inför 2026 präglas av tre samtidiga rörelser: en fortsatt industrialiserad cyberkriminalitet, en mer uttalad geopolitisk konfrontation i Europa samt ett regulatoriskt skifte som flyttar ansvar från teknikfunktion till ledningsnivå. Tillsammans förändrar detta förutsättningarna för svenska små och medelstora bolag.

Ransomware är fortsatt den mest verksamhetskritiska hottypen mot svenska organisationer (MSB 2025). Kriminella nätverk arbetar idag i specialiserade led – åtkomstförmedlare, utvecklare, förhandlare och operatörer – vilket gör angreppen skalbara och effektiva. Automatiserade verktyg söker kontinuerligt efter exponerade system, svaga autentiseringslösningar och kända sårbarheter. Det innebär att angrepp i hög grad drivs av sannolikhet att lyckas snarare än av selektiva offerurval. Det är helt enkelt mängden sårbarheter och bristande beredskap som styr.

Samtidigt har AI och automatisering sänkt tröskeln för mer träffsäkra bedrägerier. Phishingkampanjer är mer språkligt övertygande, röst- och videomanipulation används i ekonomiska bedrägerier och angripare kan snabbare analysera insamlad information för att identifiera svaga punkter (ENISA 2025). För svenska organisationer innebär detta att traditionella skyddsåtgärder – exempelvis enbart tekniska åtgärder – inte längre är tillräckliga. Angrepp sker i skärningspunkten mellan teknik och mänskligt beteende. Vi måste flytta mindset från *"att förhindra"* till *"att vara förberedd"*.

Parallellt ser vi en tydlig ökning av leverantörsrelaterade incidenter. I stället för att angripa varje organisation individuellt riktas angrepp mot gemensamma tjänsteleverantörer, SaaS-plattformar eller driftpartners. Ett intrång hos en leverantör kan därmed få spridningseffekter i hundratals verksamheter.

Den svenska incidenten kopplad till Miljödata (augusti 2025) är ett tydligt exempel på hur en leverantörsattack kan skapa bred påverkan i många verksamheter. Angreppets konsekvens låg inte bara i den tekniska påverkan, utan i beroendet. När en central tjänst slås ut påverkas hela värdekedjan.



För IT-chefer innebär detta ett strategiskt skifte: säkerhet kan inte längre definieras enbart inom den egna IT-leveransen. **Den måste förstås i ett ekosystem.**

Den geopolitiska dimensionen förstärker denna utveckling. Enligt MUST (Årsrapport 2025) befinner sig Sverige i ett försämrat säkerhetspolitiskt läge där cyberdomänen är ett etablerat verktyg för statliga aktörer. Cyberangrepp används som del av hybridpåverkan – för underrättelseinhämtning, destabilisering och strategisk positionering.

Säkerhetspolisen (2025) lyfter samtidigt att främmande makt systematiskt inhämtar information från svenskt näringsliv, särskilt inom teknik, industri, energi och samhällsnära verksamhet. Det är viktigt att förstå att denna typ av angrepp inte alltid märks. De kan vara långsiktiga, lågintensiva och fokuserade på informationsinhämtning snarare än omedelbar störning.

Detta innebär att hotbilden mot svenska företag inte enbart är direkt ekonomiskt driven. För de flesta små och medelstora bolag är sannolikheten att bli direkt utpekade i en avancerad statlig cyberoperation låg. Den relevanta risken ligger i stället i indirekt exponering – genom leverantörskedjor, teknikberoenden och långsiktig informationsinhämtning där mindre aktörer kan utgöra en intrångspunkt i ett större sammanhang.

Sverige är i detta perspektiv ett särskilt attraktivt mål. Landet är en av världens mest digitaliserade ekonomier, med hög IT-användning och omfattande digital integration i samhällsfunktioner. Samtidigt är näringslivet teknikintensivt och innovationsdrivet, med en stor andel nischade SME som utvecklar avancerade produkter och tjänster. Kombinationen av hög digital mognad och stark internationell integration innebär både konkurrenskraft och exponering.

Den svenska SME-strukturen förstärker denna exponering. Många bolag är underleverantörer till större koncerner eller till offentlig sektor och utgör därmed en del av större värdekedjor. Angripare optimerar i regel för effekt i relation till insats och risk. I praktiken innebär det ofta att mindre eller mindre skyddade aktörer i en värdekedja blir en mer rationell intrångspunkt än den primära huvudaktören.

Ett förändrat säkerhetsläge och ett mer strukturerat cyberhot

I ”Den kriminella spelplanen” beskriver Stöldskyddsföreningen hur organiserad brottslighet genomgår samma digitala omställning som näringslivet.

Traditionella brott som utpressning och bedrägerier har flyttat in i en digital miljö där verksamheten kan skalas, automatiseras och bedrivas över nationsgränser. Samtidigt minskar den fysiska risken för gärningspersonen och den potentiella vinsten ökar genom att flera offer kan angripas parallellt.

Cyberkriminalitet är därmed inte en ny typ av brott – utan en mer effektiv version av etablerade kriminella affärsmodeller i en digital ekonomi.

Vad innebär detta för små- och medelstora bolag?

För de flesta svenska SME är den största risken inför 2026 troligen inte att bli specifikt utpekade av en avancerad statlig aktör. Den största risken är fortsatt att vara tillräckligt sårbara för att bli ett rationellt val för en alltmer automatiserad cyberkriminalitet – samtidigt som man ingår i leverantörskedjor som gör verksamheten strategiskt relevant.

En återkommande svaghet hos mindre och medelstora bolag är felaktig hotbildsbedömning. Antagandet att ”vi är för små för att vara ett intressant mål” leder till underinvestering i grundläggande säkerhetsåtgärder. Ett antagande som kan stå sig dyrt. I praktiken är det just denna kombination – begränsade resurser, hög digitalisering och bristande systematik – som gör segmentet attraktivt.

Resursbegränsningar är en realitet. Många IT-chefer i SME ansvarar både för drift, utveckling, leverantörskontakter och säkerhet. Det lämnar begränsat utrymme för strukturerad riskhantering, kontinuitetsplanering och leverantörsgranskning. Samtidigt ökar beroendet av externa driftpartners och molntjänster, vilket gör organisationen känslig för händelser utanför den egna kontrollen.

Sårbarheten tar sig också olika uttryck beroende på verksamhetens affärsmodell och beroenden. I verksamheter där produktion eller leverans är tidskritisk kan ett avbrott snabbt få direkta ekonomiska konsekvenser, inte bara genom utebliven omsättning utan genom avtalsbrott och förlorade kundrelationer. I kunskaps- och tjänstebolag är istället förtroende och informationsintegritet centrala tillgångar – ett e-postintrång eller ett manipulerat betalningsflöde kan få oproportionerligt stora effekter i relation till bolagets storlek.

För bolag med kundnära digitala tjänster är tillgången till personuppgifter och betalningsinformation en affärskritisk komponent, där incidenter snabbt blir publika och varumärkespåverkande.

Därutöver möter många SME ökade säkerhetskrav genom sina kundrelationer, särskilt när de verkar i eller nära större koncerner eller offentlig sektor. Säkerhetskrav i upphandlingar och leverantörsavtal blir därmed en indirekt riskfaktor – inte för att de i sig skapar hot, utan för att bristande säkerhetsmognad kan leda till försämrad konkurrenskraft och i förlängningen affärsförlust.

Parallellt förändras spelreglerna genom ny reglering. NIS2 och den svenska Cybersäkerhetslagen innebär skärpta krav på riskhantering, incidentrapportering och ledningsansvar. Även bolag som inte direkt omfattas påverkas indirekt genom krav från kunder och större samarbetspartners. EU:s Cyber Resilience Act skärper dessutom kraven på säker produktutveckling, vilket påverkar teknik- och produktbolag i leverantörsledet.

Det regulatoriska skiftet innebär att cybersäkerhet inte längre kan hanteras enbart operativt inom IT. Styrelse och ledning får ett tydligare ansvar. För IT-chefen innebär detta en förändrad roll – från teknisk förvaltare till strategisk riskrådgivare.

Samlad bedömning inför 2026

Hotlandskapet inför 2026 kännetecknas inte av radikalt nya angreppsmetoder. Det kännetecknas av ökad systematik, ökad automatisering och ökad geopolitisk laddning. Konsekvenserna av bristande motståndskraft har blivit större, snabbare och mer affärskritiska.

För svenska SME innebär detta att säkerhet inte kan reduceras till en teknisk fråga om brandväggar och antivirus. Det handlar om att förstå sin roll i ett större ekosystem – leverantörskedjor, kundrelationer och ett förändrat säkerhetspolitiskt läge.

Den avgörande frågan inför 2026 är därför inte om hoten ökar – utan om organisationens grundläggande motståndskraft är dimensionerad för en mer systematiserad och affärsmässigt driven hotbild. För IT-chefen innebär detta ett skifte från reaktiv hantering till strukturerad riskstyrning, tydlig prioritering och en förmåga att översätta cyberrisk till affärsrisk.

Kapitel 3

Hotaktörerna och deras metoder

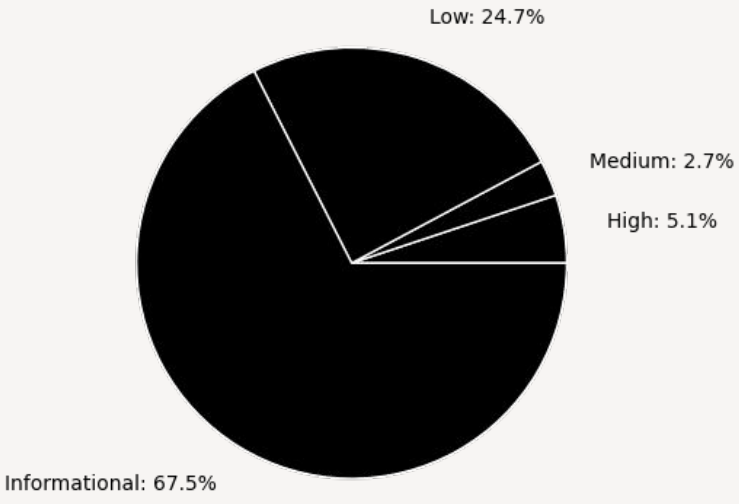
Attacker och mönster 2025

Huvudskribent
Viktor Sjögren, Cybersäkerhetsexpert, Dizparc Jönköping

Övergripande bild: vad vår SOC såg

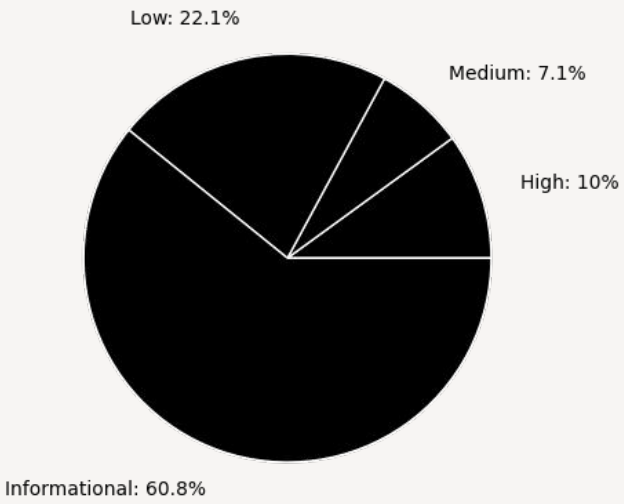
Under 2025 hanterade vårt SOC-team en stor volym incidenter från våra kunders miljöer. Av dessa klassificerades 6,6 procent som True Positives. Även om detta kanske verkar lågt är det ett realistiskt tal för en SOC. Det stora flertalet händelser är legitim nätverkstrafik, förväntade händelser och korrekta konfigurationer som triggat larm.

Allvarlighetsgraden bland samtliga incidenter fördelade sig enligt följande:



Majoriteten av all aktivitet är alltså av informationskaraktär, vilket är förväntat vid denna typ av övervakning. Det är i de övre skikten, High och Medium, som den verkliga risken koncentreras.

Bland bekräftade True Positives fördelade sig allvarlighetsgraden annorlunda:



Andelen High och Medium är alltså väsentligt högre bland bekräftade incidenter än bland totalvolymen, vilket visar att vår analys- och filtreringsprocess effektivt koncentrerar de allvarligaste hoten.

Vi använder MITRE ATT&CK som ramverk för att klassificera och analysera incidenter. Ramverket beskriver hur angripare arbetar i olika steg, från initial åtkomst till vidare rörelse och exploatering, och används både för att strukturera vår analys och för att utveckla detektionsförmåga i våra kundmiljöer.

Den dominerande angreppsvägen inom Initial Access var phishing (T1566), som stod för 46 procent av alla observationer. Att phishing fortsatt dominerar bekräftas även av både ENISA Threat Landscape 2025 och Microsoft Digital Defense Report 2025. E-post i inkorgen är fortfarande den billigaste, snabbaste och mest skalbara vägen in för en angripare.

Nyckelinsikt

Många IT-miljöer byggs enligt principen "hard shell, soft center". I våra SOC-observationer under 2025 ser vi dock att skalet sällan krackar, det kringgås. Ett klick i inkorgen eller en oåtgärdad edge-enhet räcker. När angriparen väl är inne är tystnaden det som får incidenten att växa.

Phishing i ny skepnad: multi-stage, AI och AiTM

Phishing är inte längre en enkel operation där en angripare skickar ett simpelt mail med en malware-bilaga. Phishing 2025 är sofistikerat, flerstegat och accelererat av artificiell intelligens.

Vi identifierade två särskilt oroande trender.

Multi-stage phishing med session cookie theft (AiTM)

Av vår phishing-aktivitet klassificerades 21,7 procent som credential phishing. Merparten fångades av automatiska filter, men en betydande andel krävde manuell klassificering av våra analytiker.

En mindre men högst betydelsefull grupp var AiTM-relaterade incidenter. Automatisk klassificering fångade bara ett fåtal, men vi observerade ett väsentligt större antal manuellt under året. AiTM (Adversary-in-the-Middle) är en teknik där angripare fångar upp session cookies mellan användare och legitima tjänster för att helt kringgå MFA. En användare autentiseras korrekt, men angriparen stjäl cookien och har plötsligt full åtkomst utan att ha vetat lösenordet.

AI-skriven phishing: högre kvalitet, högre click rate

Vår andra observation är att phishing-innehåll har blivit markant bättre. AI-genererad text är svårare att skilja från legitima meddelanden. ENISA Threat Landscape 2025 konstaterar att över 80 procent av phishing-kampanjer nu använder AI för att generera innehåll, och Microsoft Digital Defense Report 2025 visar att AI-drivna förfalskningar ökade med 195 procent globalt. Samma rapport visar att AI-genererad phishing har upp till 4,5 gånger högre click rate än traditionell phishing. Vi ser samma utveckling i vår SOC: användare klickar på mail som ser överraskande autentiska ut.

Det finns en djupare dimension i detta. Vi använder själva AI för att skriva mail, rapporter och texter i vardagen. Det innebär att vi alla har blivit inlärda att läsa och acceptera AI-genererat språk som normalt. Det som för några år sedan stack ut som "konstigt formulerat" ser idag ut som ett helt vanligt mail. Hotaktörer behöver inte längre lägga tid på att personlighetsanpassa sin social engineering, för mottagaren är redan van vid att läsa texter som en AI har skrivit. Vi har i praktiken tränat oss själva att inte reagera.

Volymökningen vi sett sedan 2022 drivs till stor del av denna automatisering. Phishing-relaterad aktivitet har ökat kraftigt varje år, med en mångdubbling mellan 2024 och 2025.

Nyckelinsikt
AI gör phishing både billigare och effektivare, det är väl dokumenterat. En mindre undersökt reflektion från vår SOC: vi har alla vant oss vid att läsa AI-skriven text. Det gör oss blinda för just den typ av innehåll som angripare nu producerar i stor skala.

Den kompromitterade avsändaren:
när förtroendet blir en attack

En av årets tydligaste observationer var en förändring i hur angripare använder kompromitterade organisationer för vidare angrepp.

Traditionell tanke

En angripare hackar ett företag för att stjäla data eller installera ransomware. Det är slutmålet.

Verkligheten 2025

En angripare hackar företag A för att använda det som en språngbräda för att attackera företag B och C. Offret vet inte att det är offer.

Vår statistik visade en betydande andel incidenter klassificerade som "Redirected", det vill säga mail från legitima avsändare (företag vi känner igen, ofta inom våra kunders nätverk) som innehöll phishing-länkar. Det viktigaste: vi ringde ofta upp dessa organisationer och meddelade dem att de hade blivit kompromitterade. Många visste det inte. De hade ingen insyn i sin egen e-postmiljö.

För SME-miljöer blir detta särskilt farligt. En användare ser ett mail från ett känt företagsnamn, ofta en leverantör, ett partnerföretag eller någon inom samma bransch, och klickar mycket mer villigt än på ett okänt mail.

Angripare vet detta. De använder era etablerade relationer mot er.

Nyckelinsikt
När ett mail ser ut att komma från en bekant avsändare är misstänksamheten nästan noll. Angripare vet det och använder hackade e-postmiljöer för att nå sina faktiska mål bakom er förtroendelinje.

BEC med kort tidslinje: från klick till attack på minuter

Business Email Compromise (BEC) är klassiskt: en angripare skickar ett falskt mail från ett chefskonto och och lurar någon att betala eller dela data. Fram till nyligen krävde det tålamod och handpåläggning från angriparens sida.

Det är inte längre sant.

Under året observerade vi BEC-attacker med kort tidslinje från första phishing-klick till nästa attackfas. Ett typiskt mönster:

1. Användare klickar på phishing-länk (via AiTM eller direct compromise)
2. Angripare får åtkomst till e-postkonto
3. Angripare ställer in inbox rules för att dölja sina aktiviteter
4. Inom 14 till 30 minuter skickas nya phishing-meddelanden ut från det kompromitterade kontot till organisations- eller kundlista

Branschdata visar att regler för inkorgen installeras inom 14 minuter efter kompromettering. Vi ser samma sak i vår SOC. Detektionsfönstret för SOC:ar krymper. Manuell respons räcker inte. Automation måste fånga detta innan nästa steg.

AI accelererar dessa tidslinjer ytterligare genom att automatisera ″reconn-aissance″ och “evasion″-faserna i "MITRE ATT&CK".

Nyckelinsikt
Tidslinjen från första klick till fullskalig attack är nu ofta under 30 minuter. Traditionell manuell incident response kommer inte att räcka. Automation och realtidsbedömning är inte längre valfritt.

Sårbarheter och patchning: ett tempo som inte hänger med

Under första halvåret 2025 identifierades 1 773 sårbarheter med CVSS-värden mellan 9,0 och 10,0 (kritiska). Det är ett högt tal. Många av dessa utnyttjades i det vilda inom dagar eller veckor efter att de offentliggjorts.

Vad ser vi bland våra SME-kunder?

Patchningsbeteendet förändras inte. Samma Windows-versioner som var föråldrade 2024 är fortfarande föråldrade 2025. Edge devices som VPN-gateways, proxyservrar och lastbalanserare uppdateras än mindre frekvent.

"Microsoft Digital Defense Report 2025" visar på en 800-procentig ökning i attackaktivitet riktad mot VPN- och edge-funktioner under 2025. En del av detta drivs av nya sårbarheter i dessa enheter, men det drivs också av att organisationer helt enkelt inte patchar.

AI snabbar dessutom på exploit-utveckling. Det tar nu mindre tid att skapa en fungerande exploit för en ny CVE. Angripare utnyttjar detta.

För SME utan dedikerad IT-säkerhet blir detta en omöjlig balansgång: du kan inte patcha allt, du vet inte vilka patchar som är kritiska, och du har inte tid.

Nyckelinsikt
Fler kritiska sårbarheter, stagnerande patchning och AI-accelererad exploit-utveckling. Tiden mellan "sårbarheten är känd" och "jag är kompromitterad" blir kortare.

Återkommande svagheter hos SME

Efter ett helt år av detektion och incident respons bland svenska SME ser vi ett återkommande mönster av svaga punkter. Dessa handlar sällan enbart om teknik. De är ofta strukturella.

1. Bristande övervakning av skadligt beteende i e-postmiljön

De flesta SME har inget sätt att upptäcka om deras e-postkonton används för att skicka phishing, vilka mail som faktiskt skickas från sitt domännamn, vem som hade åtkomst när, eller vad som stoppades av gateways. Allt detta hanteras ofta av en IT-leverantör "någonstans", och ingen från organisationen själv har sett loggarna på månader eller år.

Resultat: en stor andel av våra "Redirected"-incidenter var okända för avsändarorganisationen tills vi ringde upp och berättade.

2. MFA utan rätt konfiguration

MFA finns ofta, men inte överallt. E-post saknar ofta MFA. VPN har ibland bara TOTP (Time-based One-Time Password), som är lätt för AiTM att kringgå. Sällan finns härdning av "session lifetime" eller geografisk kontroll.

3. Bristande detektionsberedskap

Många SME har ingen SIEM eller SOC-övervakning. De köper antivirus, utgår från att det borde räcka, och när en incident inträffar är det redan för sent.

4. Felaktig prioritering av arbetsbelastningen

Patchning, uppdateringar och baseline-åtgärder är tråkiga. De blir inte gjorda. Istället fokuseras resurser på nya funktioner eller mer synliga projekt.

Brist på incident respons-förberedelse

Många SME har ingen plan för vad som ska hända om en attack lyckas. De saknar IT-krisplan, teknik för forensik, inget team tränat i respons, och ingen kommunikationsplan. När incidenten inträffar kastas allt i luften.

Nyckelinsikt
Tekniken är sällan problemet. Problemet är brist på processer, insyn och prioritering. En kompromitterad organisation kan existera veckor eller månader utan att organisationen själv är medveten. Vi ringde upp hackade företag och de visste inte om det. Det säger allt.

Sammanfattning: 2025 års attacklandskap

Vår data bekräftar vad internationell branschdata visar: Phishing dominerar. Phishing är mekaniserad, AI-driven och mer effektiv än tidigare. Angriparnas tidslinjer krymper. Sårbarheter ökar snabbare än patchar. Och många SME har ingen insikt i vad som faktiskt händer i sina miljöer förrän det är för sent.

Det finns en väg framåt, men den kräver fokus på de grundläggande sakerna: synlighet, respons och prioritering av försvar innan en attack redan är här.

Offensiv Verifiering: Strategiska insikter från ett simulerat angrepp

Huvudskribent

Erik Pettersson, Cybersäkerhetsexpert, Dizparc Karlstad

Emulering av Storm-0501: En anonymiserad operationsberättelse

Bakgrund

Under sensommaren 2025 genomförde hotaktören Storm-0501 ett antal uppmärksammade angrepp som fick stor spridning i branschmedia. Kampanjen markerade en tydlig evolution i aktörens tillvägagångssätt – från traditionell endpoint-ransomware till molnbaserade angrepp där Microsofts egna plattformsfunktioner användes för att exfiltrera data, förstöra säkerhetskopior och utpressa drabbade organisationer.

Mot bakgrund av dessa händelser kontaktades vårt Red team av en kund med en tydlig ambition: de ville att vi skulle genomföra en operation som emulerade Storm-0501:s tillvägagångssätt mot deras egen miljö. Syftet var dels att förstå hur organisationens befintliga skydd och processer skulle hantera den typen av angrepp, dels att identifiera konkreta förstärkningsåtgärder mot avancerade och ihärdiga hot.

Vårt första steg var att kartlägga allt tillgängligt material om Storm-0501:s faktiska angrepp.

Det arbetet visade sig vara mer utmanande än förväntat – källmaterialet var glest, utspritt och ofta i form av andra- eller till och med tredjehandsinformation. Att pussla ihop ett trovärdigt angreppsflöde krävde omfattande analys och ett antal kvalificerade antaganden.

Till slut lyckades vi konstruera ett angreppsflöde som vi bedömer efterliknar det riktiga angreppet tillräckligt väl för att ge operationen ett realistiskt underlag. Det som följer nedan är en genomgång av hur vår operation genomfördes.

Steg 1: Kartläggning och initial åtkomst

Med vetskapen om att Storm-0501 besitter djup kunskap om Azuremiljöer och att deras föredragna intrångsväg ofta kretsar kring osäkra applikationer och tjänster i Azure, inledde vi operationen med att kartlägga målets externa exponering. Med hjälp av open source-verktygen subfinder och puredns genomförde vi en subdomänskartläggning som resulterade i en förhållandevis liten mängd domäner kopplade till huvuddomänen. Den begränsade mängden gjorde det möjligt för oss att manuellt undersöka varje enskild domän för att förstå dess syfte och funktion.

En av domänerna stack ut – en hjälpsida som uppenbarligen interagerade med backendsystem. Vid granskning av sidans JavaScript-filer upptäckte vi referenser till vad som visade sig vara applikationer hostade på Azure App Services. Vi började titta på dessa och identifierade relativt snabbt en sårbarhet i en applikation som gjorde det möjligt att tvinga den att skicka anrop till godtyckliga adresser, en sårbarhetsklass som vanligen kallas Server-Side Request Forgery (SSRF).

Genom att utnyttja denna sårbarhet kunde vi stjäla en autentiseringstoken mot Azures resurshanteringsplan (management.azure.com). Med hjälp av standardverktyg för webbinteraktion och Azure-administration – curl respektive az-cli – kunde vi fastslå att tokenen gav oss åtkomst till ett generellt lagringskonto som organisationen använde för att tillhandahålla material till sin hjälpportal.

Steg 2: Eskalering via lagringskontot

En teknik som förknippas med Storm-0501 är att lista åtkomstnycklar för lagringskonton i Azure. Anledningen är enkel: dessa nycklar ger fullständig administrativ åtkomst till det aktuella lagringskontot. Med den token vi stulit i föregående steg kunde vi lista åtkomstnycklarna och konstaterade att vi hade tillgång till två stycken. Vi använde nycklarna för att lista de containers som var kopplade till lagringskontot, vilket avslöjade en stor mängd data med uppenbart skilda syften – långt utöver det material som var kopplat till hjälpsidan vi ursprungligen identifierat.

Med kommandot az storage blob list kartlade vi innehållet och noterade en hel del potentiellt intressant data. I en incidentrapport från Microsoft beskrevs hur Storm-0501 använt verktyget AzCopy för att exfiltrera data ur drabbade miljöer. För att emulera detta beteende använde vi az-kommandot på motsvarande sätt. Vid genomgång av den tillgängliga datan hittade vi uppgifter för ett automatiseringskonto – ett användarnamn med tillhörande lösenord.

Vi noterade att det fanns en risk att kontot redan hade migrerats till Managed Identities, då Microsoft vid den här tidpunkten ännu inte hade infört sitt krav på MFA för alla Azure-inloggningar med användarkonton men signalerat att det var på väg. Vi är dock simpla människor: får vi ett lösenord provar vi det. I det här fallet lyckades vi autentisera oss med kontot och kunde erhålla nya tokens.

Steg 3: Fullständig kompromiss och åtgärder

Med våra nya tokens hade vi hittat rent guld. Kontot vi kapat användes för att utföra en rad högprivilegierade åtgärder i organisationens miljö. Vi verifierade de exakta behörigheterna och konstaterade att kontot hade tilldelats Files.ReadWrite.All och Sites.ReadWrite.All.

Det visade sig att kontot var en del av en backuplösning som organisationen nyttjade – vilket innebar att vi nu hade skriv- och läsåtkomst till i princip all lagrad data. Vi befann oss i exakt den position som Storm-0501 typiskt tar sig till innan de exfiltrerar all data, tar bort säkerhetskopior och raderar information i den drabbade miljön. Med den vetskapen avbröt vi den offensiva delen av operationen och kontaktade kunden för att redogöra för angreppskedjan.

Efter avslutad operation satte vi oss ned tillsammans med kunden och deras övervakningsfunktion för att omsätta resultaten i konkreta förbättringar: vi byggde robusta detektioner anpassade efter de tekniker vi använt, etablerade processer för att systematiskt identifiera exponerade hemligheter både internt och i externt exponerade resurser, samt påskyndade organisationens pågående arbete mot en robustare identitetshantering.

Insikter från Red Team: Trender och lärdomar

Huvudskribent
Erik Pettersson, Cybersäkerhetsexpert, Dizparc Karlstad

EDR och **detektionsförmåga**

En av våra tydligaste observationer under året är att standarduppsättningar av EDR-lösningar sällan utgör ett reellt hinder vid riktade angrepp. I miljöer där försvarsorganisationen inte aktivt arbetar med att förstå och upptäcka aktuella angreppsmetoder – där ingen systematiskt söker efter avvikelser och följer upp dem – kan vi i de flesta fall nå våra mål utan att bli stoppade. Det är lätt att dra slutsatsen att verktygen är problemet, men vår erfarenhet pekar åt ett annat håll. Grundorsaken är nästan alltid brister i det övergripande cybersäkerhetsarbetet: governance, systematik och uppföljning. Ofta i kombination med en övertro på att tekniska verktyg i sig levererar skydd.

Kärnan i utmaningen är att våra metoder som red team är utformade för att efterlikna legitim verksamhet – och en EDR som saknar kontext kan inte skilja dem åt. Ta schemalagda jobb som exempel: en EDR kan inte larma varje gång ett sådant skapas eller ändras utan att generera en ohållbar mängd brus. Det som krävs är en organisation som bedriver ett aktivt säkerhetsarbete med kontextuell förståelse och en helhetsbild av hur miljön faktiskt borde fungera.

AI-driven beteendeanalys och adaptiv detektering kommer sannolikt att höja golvet för vad verktygen kan fånga på egen hand, men samma teknik är tillgänglig för angriparen – och det grundläggande problemet kvarstår: utan människor som förstår sin miljö och aktivt söker efter det som inte hör hemma där förblir tekniken otillräcklig. Det är vår övertygelse att den dynamiken kommer att bestå inom överskådlig framtid.

Cybersäkerhet är i grunden en konflikt mellan människor som utspelas på IT-arenan, och i den konflikten är det fortfarande människor och processer som avgör utfallet – inte produkter.

Least privilege och åtkomstkontroll

Brister i åtkomstkontroller och efterlevnad av least privilege är ett genomgående fynd hos nästan alla organisationer vi testar. Det tar sig olika uttryck: obehöriga med åtkomst till känsliga dokument, användare med tillgång till system som borde skyddas bakom betydligt robustare kontroller, och i flera fall hela organisationer med fullständig åtkomst till varandras lagringsytor.

Vi har även sett dokument märkta med skyddsklass ligga öppet tillgängliga för allmänheten. Gemensamt för dessa brister är att de inte beror på avsaknad av tekniska möjligheter att begränsa åtkomst – verktygen finns. Problemet är att organisationen inte har gjort det grundläggande arbetet med att inventera och förstå sin datamängd och sina åtkomster. Utan en tydlig bild av vilken data som finns, var den lagras, hur känslig den är och vem som faktiskt behöver åtkomst till den, blir varje teknisk kontroll en gissning.

Det krävs tydlig styrning och ett kontinuerligt arbete med att klassificera den data som skapas i organisationen – inte som ett engångsprojekt, utan som en löpande del av verksamheten. AI och andra tekniska framsteg har god potential att underlätta den processen avsevärt, exempelvis genom automatiserad klassificering och anomalidetektering i åtkomstmönster. Men precis som med detektionsförmågan gäller samma princip: det systematiska arbetet måste finnas på plats först.

Tekniken kan förstärka ett fungerande arbetssätt, men den kan inte ersätta ett som saknas.

Hotmodellen för molntjänster

Ett återkommande fynd är att organisationer har ett grundläggande missförstånd kring hotmodellen för molntjänster. Många verksamheter förlitar sig idag på en bred flora av molnbaserade tjänster; Microsoft 365 för kontorsapplikationer, Azure för infrastruktur och diverse SaaS-lösningar för CRM, affärssystem och ärendehantering.

Det är en helt normal bild, men den innebär en fundamentalt annorlunda hotmodell som alltför sällan beaktas.

I en molnvärld är hela poängen att resurser ska vara åtkomliga från hela världen över internet. Det betyder att identiteten är den nya gränsen mot omvärlden, inte brandväggen eller det fysiska nätverket. Trots det ser vi gång på gång att organisationer inte ställer krav på att enheter som ansluter till deras molntjänster är godkända och kontrollerade. De vanliga argumenten handlar om att man inte vill begränsa verksamheten eller kväva kreativitet genom strikta säkerhetspolicyer. Det är givetvis en avvägning varje verksamhet behöver göra utifrån sin specifika hotbild, men för oss är saken enkel: är man det minsta oroad för kontokapning så är den enda rimliga vägen framåt att nyttja de kontroller som redan finns inbyggda i moderna molnplattformar och begränsa åtkomst till organisationens egna enheter.

Perspektivet kan göras konkret: om man tillåter anställda att nå sin e-post från en privat dator hemma, tillåter man i förlängningen att en statlig hotaktör kan göra samma sak med numera triviala metoder.

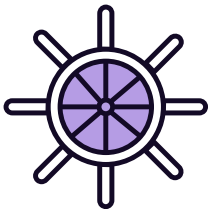
Det är inte en teknisk begränsning som saknas, kontrollerna finns. Det är återigen en fråga om governance och policy

Insikter från Red Team: Trender och lärdomar

Sammanfattning

Vår generella uppfattning efter 2025 års red team-operationer är att de flesta organisationer är överdrivet taktiska i sitt cybersäkerhetsarbete. Det finns sällan strategiska planer för hur cyberrisker ska hanteras, och ofta har man inte ens genomfört en grundläggande kartläggning av vilka risker den nuvarande miljön faktiskt exponerar verksamheten för. Konsekvensen är förutsägbar: utan en tydlig riskbild blir det omöjligt att fatta informerade beslut om vilka åtgärder som på ett rimligt sätt reducerar riskerna.

Vi har sett organisationer med hundratals odokumenterade externa resurser, administrativa portaler skyddade enbart med lösenord exponerade direkt mot internet och miljöer där externa konsultkonton sitter på nycklar till hela kungariket. Vi vet att det inte beror på bristande kompetens, tvärtom träffar vi dagligen extremt kunniga och drivna administratörer och arkitekter.



Det som saknas i de allra flesta fall, och som löper som en röd tråd genom samtliga punkter vi beskrivit ovan, är någon som tar ägarskap för riskhanteringsfrågan inom de digitala lösningarna.

IT:s mandat är, och bör vara, att leverera tekniska lösningar som driver verksamheten framåt och skapar möjligheter att lösa de problem organisationen existerar för att lösa.

Men det mandatet måste balanseras med en säkerhetsfunktion vars uppgift det är att hantera den ytterst mänskliga konflikt man utsätter sig för, vare sig man vill det eller inte, i samma stund som man nyttjar digitala lösningar.

Kapitel 4

Lärdomar, upptäckter och rekommendationer

Trendbrott och överraskningar 2025


Huvudskribenter
Viktor Sjögren, Cybersäkerhetsexpert, Dizparc Jönköping
Johan Nilsson, Cybersäkerhetsexpert, Dizparc Karlstad

De viktigaste lärdomarna från 2025 handlar mindre om nya hot och mer om hur snabbt etablerade metoder har mognat.

Phishing slutade vara ett enskilt steg

Den största förskjutningen under året var inte att phishing ökade i volym, utan att den förändrade karaktär. Det vi mötte 2025 var kampanjer med flera steg, där varje steg byggde på det föregående. En kompromitterad användare blev en betrodd avsändare, som i sin tur öppnade dörren till nästa organisation. Den kedjan var sällan synlig förrän vi aktivt letade efter den.

AI förändrade inte hotbilden, den förändrade skalan

AI-genererad phishing var ingen överraskning i sig. Det som överraskade var hastigheten. Kvaliteten på phishing-innehåll förbättrades snabbare än vi förväntade oss, och det mest oroande är att traditionella filter inte hänger med. AI-genererad text passerar regelbaserade kontroller eftersom den inte innehåller de mönster som filtrena letar efter.

Detektionsfönstret krympte snabbare än processerna

BEC-tidslinjer på under 30 minuter var inte ovanliga. Det utmanade inte bara teknik utan hela sättet vi tänker kring eskalering. Organisationer med tydliga processer och automation klarade sig. De utan stod ofta med en redan spridd attack innan första beslutet var fattat.

Mognaden var lägre än vi trodde

Den mest oväntade upptäckten var hur många av de incidenter vi hanterade som rörde organisationer som inte alls visste att de var kompromitterade. Inte för att hoten var sofistikerade, utan för att det saknades grundläggande insyn. Det visar att gapet inte primärt är tekniskt utan strukturellt.

Nyckelinsikt
2025 är året när multi-stage phishing, AiTM och kompromitterade avsändare blev norm snarare än undantag. Försvar i endast ett steg räcker inte längre.

Vad som fungerar och vad som inte gör det

Från ett SOC-perspektiv har vi möjligheten att se både vad som förhindrar incidenter och vad som bara fördröjer dem. Här är vad data säger.

Försvar med bäst effekt hos våra kunder

MFA: kritiskt men inte tillräckligt ensamt

Multifaktorsautentisering är fortfarande basen. Vi ser att organisationer utan MFA möter betydligt högre credential compromise rate. Men traditionell MFA (SMS, TOTP) bryts rutinmässigt genom AiTM-attacker. Phishing-resistent MFA, det vill säga FIDO2 och passkeys, stannar attack chain vid punkt två. Vi rekommenderar FIDO2 för alla externa tjänster, särskilt Microsoft 365, Azure och VPN.

SOC/MDR-övervakning fångar det som edge-försvar missar

Under 2025 hanterade vår SOC ett stort antal True Positive-incidenter som edge-försvaret (e-postfilter, proxy, brandvägg) inte flaggat. Det är inte edge-försvarets fel, det är designen. En angripare som redan har inloggningsuppgifter behöver inte passera edge-filtret. En lateral movement passerar brandväggen. En C2-kommunikation över HTTPS ser ut som legitim trafik. Övervakning av identiteter, autentisering och endpoint-beteende fångar dessa.

Villkorsstyrd åtkomst minskar attackytan

Geografi- och enhetsbaserade restriktioner fungerar. När en miljö konfigurerar Villkorsstyrd åtkomst (CA-policyer) som blockerar inloggning från okända länder eller enheter som inte uppfyller säkerhetskraven (Intune compliance), genomslagsgraden för komprometterade inloggningsuppgifter. Vi mäter detta i reducerat antal BEC-försök som lyckas eskalera.

Security awareness behöver omformas

Årlig compliance-utbildning? Irrelevant mot AI-phishing. Simulerad phishing-testning? Effektiv. Vi ser att organisationer som kör månatlig simulerad phishing med feedback-mekanismer reducerar click rate från cirka 35 procent till cirka 8 procent på 6 månader. Nyckeln är att det inte är en punktinsats utan en kontinuerlig process.

Processer som fungerar: snabb eskalering och playbooks

En organisation utan definierad incident respons-process tar i genomsnitt 32 dagar att detektera ett intrång, enligt ENISA. Med definierad eskaleringsprocess och phishing-playbooks reduceras tiden till timmar. Vi ser detta varje vecka när en kund med bra process stoppar en attack medan kunder utan process eskalerar den till full compromise.

Vad som INTE fungerar

Enbart edge-försvar utan övervakning är som ett lås utan larmsystem. Angriparen som redan är innanför dörren är osynlig. Manuell patchning med långa cykler (månads- eller kvartalsvis) möter 1 773 CVSS 9-10-vulnerabilities bara i H1 2025, och många utnyttjas redan aktivt innan patchfönstret har öppnats. Och tillit till att partners och leverantörer "har koll" stämmer sällan. Uppskattningsvis 30 procent av lyckade angrepp är tredjepartsrelaterade, och många offer visste inte att de var kompromettterade.

Nyckelinsikt
Tillräckligt försvar är skiktat, övervakat och snabbt. Det räcker inte att filtrera eller blockera. Du måste se vad som händer innanför nätverket och reagera på timmar, inte veckor.

Gapet mellan upplevd och faktisk säkerhet

SME-ledares överraskning återvänder ofta till samma tema: "Vi trodde vi var säkra."

"Vi är för små för att vara mål"

Branschdata visar att uppemot 88 procent av lyckade ransomware-angrepp drabbar små och medelstora företag. Siffran är överrepresenterad just för att attacker mot SME oftare lyckas. Små bolag är inte ett sidospår i attacklandskapet, de är huvudmålet. Varför? Lägre säkerhetsbudget, fokus på enskild person (VD/ekonomichef), svag backup-strategi och ofta samma teknikstack som större företag (Microsoft 365, Outlook) men utan enterprise-kontroller.

"Vi har MFA, vi är säkra"

MFA är ett starkt försvar, men AiTM attackerar genom att fånga MFA-sessionen i realtid under phishing-processen. En anställd klickar en länk, blir presenterad en legitim inloggningssida (proxy-baserad), matar in lösenord och MFA-kod, och angriparen får båda. Traditionell TOTP/SMS MFA passeras. Phishing-resistant MFA (FIDO2) kan inte kringgås på detta sätt. De blir då en lättare måltavla för hotaktören.

"Våra partners har koll"

Tredjepartsrisken är dokumenterad. Uppskattningsvis 30 procent av lyckade angrepp spåras till kompromitterad partner eller leverantörsåtkomst, enligt branschdata. Många offer var överraskade. De hade inte övervakat partneråtkomst eller verifierat att partners upprätthöll sina egna säkerhetsstandarder. En leverantör med svag MFA blir en väg in till dig.

"Vi patchar vid nästa underhållsfönster"

1 773 CVSS 9-10-Sårbarheter rapporterades bara i första halvåret 2025. Många av dessa är redan utnyttjade innan månadens andra eller tredje

underhållsfönster. Ransomware-operatörer kör automatisk scanning för kända sårbarheter. En 72-timmars policy för kritiska patchar är standard idag. Veckovis eller månatlig patchning är redan för långsamt.

"Vi har aldrig blivit hackade"

ENISA pekar på 32 dagars median detection gap, alltså tiden mellan intrång och upptäckt. Många organisationer är redan kompromitterade men vet det inte. En angripare som kommer in med inloggningsuppgifter behöver inte dölja sitt spår. En bakdörr som ligger dold kan vänta månader innan den aktiveras.

"Cybersäkerhet är för dyrt"

Enligt Verizon DBIR 2025 betalade ransomware-offer 2024 en median på 115 000 USD, vilket motsvarar ungefär 1,2 miljoner SEK. 64 procent av offren valde att inte betala alls, men även då kvarstår kostnader för utredning, driftstopp och återställning. I de större incidenter vi själva hanterat under 2025 har totalkostnaden för fullständig incident respons, forensik och uteblivna intäkter ofta hamnat i miljonklassen.

Till det ska jämföras kostnaden för kontinuerlig övervakning. En SOC/MDR-tjänst för ett medelstort företag kostar typiskt några tiotusental kronor i månaden, vilket över ett år nästan alltid är lägre än kostnaden för en enda allvarlig incident. Det är den här asymmetrin som gör proaktivt skydd billigare än reaktiv hantering, inte ett specifikt pris.

Nyckelinsikt
Uppfattningen om säkerhet baseras ofta på tur eller frånvaro av detektion, inte faktisk säkerhet. Det gapet är där incidenter växer ohindrat.

Investera nu: varför cybersäkerhet inte längre är valfritt

Investeringsgapet är reellt

Investeringsgapet är tydligt även utan globala genomsnitt, vi ser det dagligen hos svenska SME. Många av de organisationer vi möter har ingen definierad säkerhetsbudget alls. Säkerhet är något som hanteras när något går fel, inte en kostnadspost som planeras. Andra investerar i verktyg utan att samtidigt investera i förmågan att använda dem. Licenser räcker inte, någon måste läsa larmen.

ENISA:s senaste undersökningar av organisationer i Europa bekräftar bilden. I NIS Investments 2024 uppgav 34 procent av SME att de inte kan be om den extra budget som krävs för att nå en rimlig säkerhetsnivå, och 59 procent rapporterade rekryteringssvårigheter. I den nyare NIS Investments 2025 uppger 47 procent av organisationerna att de inte planerar att anställa cybersäkerhetspersonal alls de kommande två åren, och 83 procent av dessa rapporterar att det är svårt att hitta kompetens. SME rapporterar samtidigt det lägsta förtroendet för sin egen cyberresiliens av alla kategorier i undersökningen.

Det här är en viktig nyans. Det är inte så att ledningen i svenska SME inte vill investera, och det är sällan så att de saknar insikt om risken. Problemet är strukturellt: den kompetens som krävs för att bygga och driva en modern säkerhetsförmåga är svår att rekrytera, dyr att behålla, och i praktiken omöjlig att hålla igång som en intern funktion med en eller två personer. Det som krävs är snarare en budget som gör det möjligt att ta in hjälp där den interna förmågan inte räcker, kontinuerlig övervakning, incidenthantering, sårbarhetshantering och rådgivning. Budgeten är i praktiken ett sätt att kompensera för att marknaden för cybersäkerhetskompetens är vad den är.

Sverige följer samma riktning. Regeringen har de senaste åren ökat anslagen till MSB, Försvarsmakten och den nya cybersäkerhetsmyndighetsstrukturen som följer av NIS2-implementeringen. Frågan är inte längre om du ska investera, utan hur snabbt du kan stänga gapet, både gentemot det europeiska snittet och mot den hotbild vi beskrivit i rapporten.

Den asymmetriska risken är reell. En enda allvarlig incident kan kosta mer än flera års samlat säkerhetsarbete, och för ett mindre bolag kan det räcka för att skada både verksamhet och kundrelationer under lång tid. Framgångsfaktorn är sällan storleken på budgeten utan om grundläggande detektions- och responsförmåga finns på plats, i egen regi eller genom en partner.

Europa rör sig, och Sverige måste hänga med

NIS2-direktivet och DORA-förordningen förändrar spelplanen i Europa. Sveriges cybersäkerhetslag (2025:1506) trädde i kraft den 15 januari 2026 med en "whole-entity"-princip: faller din organisation inom scope måste hela verksamheten uppfylla kraven, inte bara den tjänst som triggade regleringen. Ledningsgruppen bär personligt ansvar, med sanktioner upp till 10 miljoner EUR (cirka 113 miljoner SEK) eller 2 procent av global omsättning enligt NIS2-direktivet (2022/2555).

Det här handlar inte bara om efterlevnad. Det handlar om att bygga ett gemensamt starkt Europa. Cyberhot respekterar inga nationsgränser. En kompromitterad svensk underleverantör kan vara ingången till ett europeiskt sjukhus, en dansk bank eller en finsk myndighet. Supply chain-kraven i NIS2 innebär att även SME som inte direkt omfattas kommer att möta krav från sina kunder och partners. Vi behöver alla dra vårt strå till stacken.

Enligt ENISA:s NIS Investments-rapporter allokerar europeiska organisationer i NIS-scope i snitt 9 procent av sin IT-budget till informationssäkerhet, upp från 7,1 procent 2022. Medianen för informationssäkerhetsbudgeten har fördubblats till 1,5 miljoner EUR, vilket motsvarar ungefär 17 miljoner SEK per organisation. Trenden är tydlig: regulatoriska krav och hotbild driver upp investeringarna i hela Europa. Samtidigt är gapet till USA fortfarande stort. Enligt ENISA:s 2025-rapport allokerar europeiska organisationer i snitt 41 procent mindre till cybersäkerhet än amerikanska motsvarigheter, och andelen säkerhets-FTE i IT-organisationen minskar fjärde året i rad.

Sverige följer samma riktning. Regeringen har de senaste åren ökat anslagen till MSB, Försvarsmakten och den nya cybersäkerhetsmyndighetsstrukturen som följer av NIS2-implementeringen. Frågan är inte längre om du ska investera, utan hur snabbt du kan stänga gapet, både gentemot det europeiska snittet och mot den hotbild vi beskrivit i rapporten.

Fem kritiska åtgärder för 2026

Baserat på vad vi ser fungera i praktiken, och vad hotlandskapet kräver, rekommenderar vi fem prioriterade insatser.

1. Strategiskt säkerhetsarbete: från ad-hoc till strategi

Cybersäkerhetsarbete blir ofta en samling enskilda åtgärder utan tydlig riktning. En strategi handlar om att skapa just den riktningen – att utgå från risk snarare än från enskilda initiativ.

Det innebär att förstå hotbilden, identifiera relevanta sårbarheter och sätta dessa i relation till möjliga konsekvenser. Utan den kopplingen blir det svårt att avgöra vilka åtgärder som faktiskt reducerar risk.

En strategi behöver också beskriva hur arbetet ska realiseras i praktiken – vilka kompetenser som krävs, hur ansvar fördelas och hur arbetet följs upp över tid.

Vår erfarenhet, bekräftad i både incidenthantering och red team-övningar, är att bristerna sällan ligger i enskilda tekniska kontroller. Problemet är oftare att dessa delar saknas som helhet.

Cybersäkerhet blir därmed en fråga om styrning snarare än enbart teknik.

2. SOC/MDR: se vad som faktiskt händer i din miljö

24/7-monitorering av e-post, identiteter, endpoints och molntjänster är inte längre reserverat för storföretag. Det är grundförutsättningen för att överhuvudtaget veta om du är kompromitterad. ENISA pekar på 32 dagars median detection gap utan aktiv övervakning. Med en SOC/MDR-tjänst reduceras det till timmar.

Majoriteten av våra True Positive-incidenter under 2025 flaggades inte av edge-försvar. Det är inte edge-försvarets fel. Angripare som redan har inloggningsuppgifter passerar brandväggen obemärkt. Utan operativ övervakning ser du dem aldrig.

3. Korta patchcykler: 72 timmar för kritiska sårbarheter

1 773 CVSS 9-10-sårbarheter identifierades bara under första halvåret 2025. Många exploiteras i det vilda inom dagar. Ransomware-operatörer kör automatiserad scanning efter kända sårbarheter. En policy för att patcha kritiska sårbarheter inom 72 timmar, med automatiserad distribution där det är möjligt, är inte ambitiöst. Det är minimum. Edge devices som VPN-gateways och lastbalanserare kräver särskild uppmärksamhet, attackaktivitet riktad mot dessa ökade med 800 procent under 2025.

4. Verifiera leverantörers säkerhet: din kedja är bara så stark som den svagaste länken

Supply chain-risken är dokumenterad och växande. Uppskattningsvis 30 procent av lyckade angrepp spåras till kompromitterad tredje part. Siffran är överrepresenterad i just lyckade attacker, eftersom attacker mot leveranskedjan ofta ger angriparen ett förtroende som öppnar dörrar som annars hade varit stängda. Under 2025 ringde vi upp organisationer för att meddela att de hade blivit kompromitterade och användes som språngbräda mot andra. Många visste inte om det. NIS2 ställer dessutom explicita krav på säkerhet i leverantörskedjan. Börja med att kartlägga dina kritiska leverantörer, ställ konkreta krav på MFA, säkerhetsuppdateringar och övervakning, samt begär intyg eller certifieringar (som ISO 27001 eller SOC 2). Dina partners säkerhet är din säkerhet.

Investera nu: varför cybersäkerhet inte längre är valfritt

Sammanfattning

2025 är året då multi-stage phishing, AiTM och AI-genererad e-post blev norm. SME-organisationer står ofta utan tillräckligt skydd, inte för att de inte förstår risken, utan för att de undervärderar hot mot sin egen storlekskategori och övervärderar skyddet från traditionell MFA och leverantörstillit.

Europa rör sig. NIS2 och DORA ställer nya krav. Sverige har investerat mer än någonsin i nationell cybersäkerhet. Men det räcker inte om inte varje enskild organisation tar sitt ansvar. Cybersäkerhet är inte ett nollsummespel. Ett starkare försvar hos din organisation stärker hela kedjan, dina kunder, dina partners och i förlängningen det europeiska digitala ekosystemet.

Inför 2026 rekommenderar vi att börja med de fem kritiska åtgärderna omedelbart: SOC/MDR, korta patchcykler, leverantörsverifiering, strategiskt säkerhetsarbete och penetrationstester. Det är genomförbart, kostnadseffektivt och nödvändigt.

Kapitel 4

Om rapporten och Dizparcs arbete

Om rapporten

Denna rapport baseras på operativ threat intelligence från Dizparcs Security Operations Center (SOC) under 2025. Data samlas kontinuerligt från monitoreringen av våra kunders IT-miljöer och kompletteras med hotinformation från etablerade internationella källor som ENISA och Microsoft, samt annan branschdata.

All data som presenteras är fullständigt anonymiserad. Ingen enskild kund, organisation eller individ kan identifieras i materialet. Syftet med denna rapport är att bidra till ett säkrare svenskt näringsliv genom att dela kunskap om aktuella hot och trender som påverkar svenska företag och organisationer.

Dizparcs threat intelligence bygger på en kombination av teknologi och mänsklig erfarenhet.

Om Dizparcs cybersäkerhetsverksamhet

Dizparcs cybersäkerhetsdotterbolag är en del av Dizparc-gruppen och erbjuder en helhetslösning för moderna organisationers säkerhetsbehov.

SOC/MDR-tjänster: 24/7-monitorering, detektion och incident respons. Vi övervakar kunders IT-miljöer dygnet runt för att identifiera och neutralisera hot innan de orsakar skada. Vår SOC är navet i verksamheten och grunden för den threat intelligence vi producerar.

Incident Respons: När en incident inträffar agerar vi snabbt med etablerade playbooks och operativ erfarenhet från hundratals incidenter. Vi hjälper organisationer att begränsa skadan, utreda omfattningen och återställa normal drift.

Threat Intelligence: Vi bedriver löpande omvärldsbevakning och analys av hotlandskapet, med fokus på de hot som är relevanta för svenska SME. Denna rapport är ett resultat av det arbetet.

Red Teaming och penetrationstester: Vi testar organisationers försvar genom realistiska angreppsscenarier och tekniska penetrationstester. Det ger konkret insikt i var svagheter finns innan en verklig angripare hittar dem.

Strategisk rådgivning: Vi hjälper organisationer att bygga säkerhetsstrategi, prioritera investeringar och mogna sitt säkerhetsarbete utifrån faktisk risk och affärskontext.

Dizparcs cybersäkerhetsteam är baserade i Jönköping och Karlstad och fokuserar på det Microsoft-ekosystem som dominerar svenska SME-miljöer, med djup expertis inom Microsoft Sentinel (SIEM), Microsoft Defender for Endpoint och Microsoft Entra ID.

Förklaring av tekniska termer

Denna bilaga förklarar tekniska termer och förkortningar som förekommer i rapporten, för läsare som vill förstå begreppen utan att behöva söka vidare.

Ramverk och klassificeringar

MITRE ATT&CK — Ett internationellt ramverk som kategoriserar och beskriver kända attacktekniker. Används av säkerhetsbranschen globalt för att klassificera vad angripare gör i varje steg av en attack. Ramverket är uppdelat i taktiker (vad angriparen vill åstadkomma) och tekniker (hur de gör det).

T1566 (Phishing) — MITRE ATT&CK-klassificering för phishing-attacker. Numret är en unik identifierare för just denna attackteknik i ramverket. T1566 täcker all form av phishing, inklusive e-post med skadliga bilagor och länkar.

Initial Access — Den första fasen i en attack, det vill säga hur angriparen får sitt initiala fotfäste i en miljö. Phishing är den vanligaste metoden för initial access.

Pre-Attack (Reconnaissance) — Fasen innan själva attacken, där angripare samlar information om sitt mål: vilka system som körs, vilka e-postadresser som finns, vilka tjänster som är exponerade mot internet.

Defense Evasion — Tekniker angripare använder för att undvika upptäckt, till exempel att dölja sin aktivitet i legitim trafik, manipulera loggar eller använda krypterade kanaler.

Execution — Fasen där angriparen faktiskt kör skadlig kod eller kommandon i den kompromitterade miljön.

Lateral Movement — När en angripare som redan har tillgång till ett system rör sig vidare till andra system inom samma nätverk, ofta för att nå mer värdefull data eller högre behörigheter.

CVSS (Common Vulnerability Scoring System) — Ett standardiserat poängsystem för att bedöma allvarlighetsgraden hos säkerhetssårbarheter, på en skala från 0 till 10. Värden 9,0 till 10,0 räknas som kritiska.

CVE (Common Vulnerabilities and Exposures) — Ett unikt ID-nummer som tilldelas varje publikt känd säkerhetssårbarhet, till exempel CVE-2025-1234. Används som gemensamt referenssystem i hela branschen.

Attacktyper och metoder

Phishing — Social engineering-teknik där angripare försöker lura mottagare att klicka på skadliga länkar, öppna bilagor eller lämna ut inloggningsuppgifter, vanligtvis via e-post.

Credential phishing — En form av phishing specifikt inriktad på att stjäla inloggningsuppgifter (användarnamn och lösenord).

AiTM (Adversary-in-the-Middle) — En avancerad phishing-teknik där angriparen placerar sig mellan användaren och den legitima tjänsten. Användaren loggar in som vanligt och ser rätt sida, men angriparen fångar upp session cookies och får full åtkomst utan att behöva lösenordet igen. Kringgår traditionell MFA.

Multi-stage phishing — Phishing-attacker som sker i flera steg, till exempel: först kompromitteras ett företag, sedan används dess e-postkonton för att skicka phishing till nästa mål, ofta med AiTM-teknik.

BEC (Business Email Compromise) — En angripare får kontroll över ett legitimt e-postkonto (ofta en chef eller ekonomiansvarig) och använder det för att lura mottagare att göra betalningar, dela känslig data eller utföra andra åtgärder.

Ransomware — Skadlig kod som krypterar en organisations filer och kräver en lösensumma (ransom) för att återställa åtkomsten. Ofta kombinerat med hot om att publicera stulen data.

C2 (Command and Control) — En kommunikationskanal som angripare etablerar mellan ett kompromitterat system och sin egen infrastruktur, för att styra angreppet, exfiltrera data eller installera ytterligare skadlig kod.

Supply chain-attack — En attack där angriparen komprometterar en leverantör, partner eller annan tredje part för att nå sitt egentliga mål. Utnyttjar det förtroende som redan finns mellan organisationer.

Försvarsmekanismer och teknologi

SOC (Security Operations Center) — En funktion eller tjänst som övervakar en organisations IT-miljö dygnet runt för att upptäcka, analysera och hantera säkerhetsincidenter i realtid.

MDR (Managed Detection and Response) — En tjänst där en extern leverantör tillhandahåller SOC-funktionalitet, inklusive övervakning, detektion och incidenthantering, som en managed service.

SIEM (Security Information and Event Management) — En plattform som samlar in, korrelerar och analyserar loggdata från en organisations alla system för att upptäcka avvikelser och potentiella säkerhetsincidenter. Microsoft Sentinel är ett exempel på en SIEM-plattform.

MFA (Multi-Factor Authentication) — Flerfaktorsautentisering, det vill säga att inloggning kräver minst två oberoende faktorer, till exempel lösenord plus en kod från en app eller fysisk nyckel.

TOTP (Time-based One-Time Password) — En typ av MFA där en app genererar en tidsbegränsad kod (vanligtvis sex siffror) som byts ut var 30:e sekund. Säkrare än SMS men sårbart för AiTM-attacker.

FIDO2/Passkeys — En modern MFA-standard baserad på kryptografiska nycklar som är bundna till specifika webbplatser. Till skillnad från TOTP och SMS kan FIDO2 inte luras av phishing-sidor eftersom autentiseringen sker direkt mot den korrekta domänen.

Conditional Access (CA) — Policyer i Microsoft-miljöer som styr vilka villkor som måste uppfyllas för att en inloggning ska tillåtas, till exempel godkänd enhet, specifik geografisk plats eller korrekt compliance-status.

Inbox rules — Regler i e-postklienter som automatiskt hanterar inkommande mail, till exempel flytta, radera eller vidarebefordra meddelanden. Angripare skapar ofta inbox rules för att dölja sin aktivitet efter en kompromiss.

Edge device — Nätverksutrustning som sitter i gränssnittet mellan en organisations interna nätverk och internet, till exempel brandväggar, VPN-gateways, proxyer och load balancers.

Incident Response — Den strukturerade processen för att hantera en säkerhetsincident: identifiera, begränsa, utreda, åtgärda och återställa.

Red Teaming — En metodik där säkerhetsexperter simulerar verkliga angrepp mot en organisation för att testa dess försvarsförmåga. Till skillnad från penetrationstester har red teaming ofta bredare scope och kan inkludera social engineering, fysisk access och mer.

Penetrationstest — En kontrollerad attack mot specifika system eller applikationer för att identifiera sårbarheter, vanligtvis med ett definierat scope och tidsram.

Regulatoriska termer

NIS2 (Network and Information Security Directive 2) — EU-direktiv som ställer krav på cybersäkerhet för samhällsviktiga och digitala tj änster. Implementerat i svensk lag som cybersäkerhetslagen (2025:1506).

DORA (Digital Operational Resilience Act) — EU-förordning med krav på digital operativ motståndskraft för den finansiella sektorn, inklusive krav på threat-led penetration testing.

Cybersäkerhetslagen (2025:1506) — Svensk lag som implementerar NIS2-direktivet, i kraft sedan 15 januari 2026. Innebär en "whole-entity"-princip och personligt ansvar för ledning och styrelse.

Övriga termer

True Positive — En incident som efter analys bekräftas vara en faktisk säkerhetshändelse, till skillnad från False Positives (falsklarm).

Redirected (incident) — I vår SOC-klassificering: en incident där phishing-mail kommer från en legitim men kompromitterad avsändare, det vill säga en organisation vars e-postkonto har kapats och används för att sprida phishing vidare.

Click rate — Andelen mottagare som faktiskt klickar på en phishing-länk i ett utskick. Används för att mäta effektiviteten hos phishing-kampanjer och säkerhetsutbildning.

Detection gap — Tiden mellan att ett intrång sker och att det upptäcks. Enligt ENISA är medianen 32 dagar utan aktiv övervakning.

Omnämnda referenser

Branschrapporter och threat intelligence

- ENISA Threat Landscape 2025
  https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025
- Microsoft Digital Defense Report 2025
  https://www.microsoft.com/en-us/security/security-insider/threat-landscape/microsoft-digital-defense-report-2025

Svenska myndigheter och nationella källor

- MSB – Cyberangreppens utveckling 2023–2025: Årsrapport cyberincidentrapportering 2025
  https://rib.msb.se/filer/pdf/31323.pdf
- MUST – Årsöversikt 2025
  https://www.forsvarsmakten.se/aktuellt/nyheter/must-arsoversikt-2025/
- Säkerhetspolisen – Säkerhetspolisens lägesbilder
  https://www.sakerhetspolisen.se/om-sakerhetspolisen/publikationer/sakerhetspolisens-lagesbilder.html

EU-regelverk och europeiska ramverk

- NIS2-direktivet
  https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng
- DORA – Digital Operational Resilience Act
  https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng
- Cyber Resilience Act
  https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng
- ENISA NIS Investments 2024: https://www.enisa.europa.eu/publications/nis-investments-2024 ENISA NIS Investments 2025: https://www.enisa.europa.eu/publications/nis-investments-2025

Svensk reglering och strategiska dokument

- Regeringen – Ett starkt skydd för nätverks- och informationssystem: en ny cybersäkerhetslag https://www.regeringen.se/rattsliga-dokument/proposition/2025/10/prop.-20252628
- Regeringen – En ny era av cybersäkerhet: Nationell strategi för cybersäkerhet 2025–2029 https://www.regeringen.se/informationsmaterial/2025/03/nationell-strategi-for-cybersakerhet-2025-2029/

Dizparc är ett relativt ungt företag som sedan starten valt att gå vår egen väg. Till skillnad från många branschkollegor fokuserade på storstadsregionerna satsar vi på att finnas nära till hands för alla mindre och medelstora verksamheter som önskar en lokal digital partner.

På våra marknader arbetar drivna entreprenörer och deras erfarna team med att skapa nya digitala möjligheter hela vägen från affärsutveckling och rådgivning till teknisk leverans och förvaltning. Vi är måna om att bygga upp stabila partnerskap med långsiktiga relationer som bas. Vårt mål är alltid att lära känna våra kunders verksamhet på djupet för att kunna utmana och ifrågasätta gamla sanningar och skapa en så framtidssäker och konkurrenskraftig position på den digitala arenan som möjligt.

Läs mer på **dizparc.se**

Nyfiken på hur vi kan hjälpa dig?

Läs mer på dizparc.se/cybersakerhet eller
ta en förutsättningslös kontakt så pratar
vi gärna mer om just dina utmaningar.