The Cyber Resilience Guide

De 7 vanligaste säkerhetsmissarna

– och hur du förebygger dem

CYLOQ

Hotbilden förändras. Hänger din säkerhet med?

Cyberhoten utvecklas snabbare än någonsin. AI-drivna attacker, zero-days som utnyttjas inom timmar, och intrång via leverantörskedjan är inte längre något som "kan hända" – det händer hela tiden.

Enligt IBM Cost of a Data Breach Report 2025 låg mediankostnaden för ett dataintrång på 4.44 miljoner USD. En stor andel av dessa incidenter började med sårbarheter som hade kunnat förebyggas om rätt skyddsåtgärder funnits på plats. Bland de vanligaste vägarna in fanns phishing, attacker via leverantörer och tredjepart, och komprometterade inloggningsuppgifter. Samtidigt gör automatisering och AI att angrepp inte bara sker snabbare, utan också i betydligt större skala. Det leder till fler infektioner, helt enkelt för att fler träffas snabbare.

Vi på Cyloq granskar hundratals miljöer varje år. I den här guiden sammanfattar vi de sju vanligaste säkerhetsmissarna vi ser i verkligheten – både i kod och konfiguration, men också i arbetssätt, beslut och säkerhetskultur.

Etablerade ramverk som OWASP-listor är viktiga riktmärken, särskilt inom webbapplikationssäkerhet, men de täcker bara en del av bilden. I denna guide kombinerar vi dessa ramverk med observationer från verkliga attacker, tester och uppdrag. Vi lyfter både tekniska och organisatoriska brister som återkommer gång på gång – och ger dig åtgärdsförslag och tips för att och förebygga dem.

1

Felkonfigurerade system och tjänster

Felkonfigurationer är ett av de mest underskattade hoten mot IT-säkerheten. De förekommer i allt från applikationer och molntjänster till nätverksinfrastruktur och autentiseringslösningar.

I OWASP Top 10 2025 för webbapplikationer listas detta som A02: Security Misconfiguration, men problemet är inte bara begränsat till webben. Felaktiga inställningar, kvarlämnade funktioner och öppna åtkomstpunkter dyker upp i alla typer av system och miljöer.

Det räcker med en felaktig inställning i ett system, en onödigt öppen port eller en kvarlämnad debug-funktion för att öppna dörren för ett intrång.

Exempel på vad vi ofta ser:

- En öppen S3-bucket med känslig data, utan autentisering.
- Testinstanser som ligger publikt tillgängliga, med svaga lösenord.
- Adminpaneler som inte är skyddade bakom VPN eller IP-whitelist.
- Felaktiga rättigheter i molntjänster – där "alla" har läsrättigheter till allt.

Den gemensamma nämnaren är små misstag som ofta uppstått som en effekt av stress, otydliga ansvarsområden eller komplexa miljöer där ingen har full överblick. Många system byggs dessutom upp över tid, av olika personer, med olika nivåer av dokumentation, vilket gör det svårt att ha en samlad överblick. Detta är små misstag som kan leda till fullständig kompromettering av ett system.

Vad du kan göra:

Gör kontinuerliga sårbarhetsskanningar

Använd verktyg för automatiserad sårbarhetsskanning – både på kodnivå och i den exponerade infrastrukturen. Gör det löpande, inte bara vid release. Och glöm inte att även skanna test- och stagingmiljöer.

Definiera standardkonfigurationer

Definiera hur ett säkert system ska vara konfigurerat i din organisation. Det gör det lättare att upptäcka avvikelser – och att följa upp att säkerhetskonfigurationer faktiskt efterlevs i praktiken.

Ha tydliga rutiner för deployment och change management

All förändring i system ska följas upp med test. Automatiserade CI/CD-pipelines med inbyggda säkerhetskontroller minskar risken för att oavsiktliga felkonfigurationer når produktion.

Repetera, granska, dokumentera

Säker konfiguration är inte en engångsinsats. Det kräver löpande arbete, ansvarsfördelning och uppdaterade rutiner. Dokumentera inte bara vad ni gör – dokumentera också varför.

2

Bristande segmentering

Nätverkssegmentering är en av de mest grundläggande försvarsmekanismerna i moderna IT-miljöer.

Att ha en platt nätverksstruktur är som att alla dörrar till en byggnad är olåsta. Om en angripare tar sig in genom en enda sårbar punkt, till exempel en användares enhet eller en mindre skyddad server, kan de ofta röra sig fritt genom resten av infrastrukturen. Det kallas lateral rörelse, och är en vanlig metod i riktade attacker.

En angripare kan exempelvis ha fått initial access via ett gammalt externt webbgränssnitt, och inom loppet av timmar haft full access till interna HR-system, finansiell data och kundinformation. Bara för att nätverket saknade tillräcklig segmentering.

Vad du kan göra:

- Separera känsliga miljöer från användarnätverk
- Begränsa kommunikationen mellan segment med hjälp av brandväggar och policies
- Tillåt endast "need-to-know"-access mellan system
- Kombinera med Zero Trust-principer för autentisering och åtkomst

Segmentering löser inte allt. Men den kan vara skillnaden mellan en lokal incident och ett fullskaligt intrång. Genom att begränsa åtkomst väger segmenteringen upp för andra svagheter, och köper dig tid att agera.

3

Incidentrespons som bara finns på papper

De flesta organisationer har någon form av incidentplan. Den ligger i en mapp på intranätet, uppdaterades för ett par år sedan, och innehåller roller och processer som inte längre är relevanta. Och, den är aldrig testad i praktiken. Det är inte förrän en riktig incident inträffar som bristerna i planen märks, som exempelvis att:

- Roller är otydliga eller obemannade.
- Loggningen fångar inte det som faktiskt pågår.
- Kommunikationsvägar är oklara.
- Beslut tas för sent – eller inte alls.

Effekten det får är att attacken inte stoppas i tid och konsekvenserna blir enorma. Ta till exempel en organisation som utsätts för ransomware en fredag eftermiddag. IT-avdelningen försöker hantera situationen själva men har begränsad insyn i hur allvarligt det är. Säkerhetschefen kopplas in först på måndag morgon. Då har attacken redan spridit sig, backuperna är krypterade och flera affärskritiska system ligger nere.

För att se till att ni har en gedigen incidentrespons bör ni:

Simulera på riktigt

Gör tabletop-eller red teaming-övningar där olika incidenter spelas upp och teamet får fatta beslut i realtid.

Testa tekniken

Loggar ni det ni behöver? Går det larm vid rätt tillfällen? Testa och justera.

Definiera roller

Vem ansvarar för beslut, kommunikation, återställning? Det ska vara tydligt – även under stress.

Utbilda organisationen

Alla behöver inte kunna allt, men alla måste veta vad de ska göra.

4

Övertro på intern kompetens

En annan vanlig miss många organisationer gör är att förlita sig på sitt interna säkerhetsteam. För även de mest kompetenta teamen riskerar att bli hemmablinda. När man granskar samma kodbas, samma konfigurationer och samma miljöer dag ut och dag in, är det lätt att förbise det som inte sticker ut, trots att det är just där hoten ofta gömmer sig.

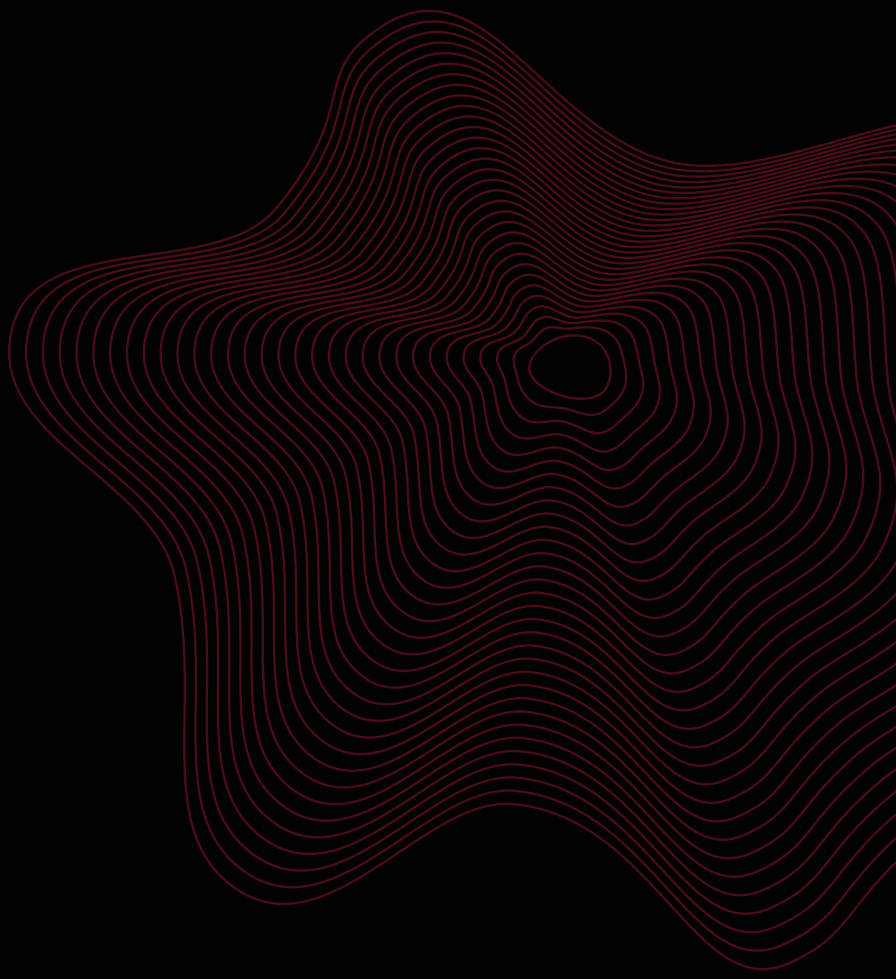
Dessutom tenderar många organisationer att överskatta sin egen säkerhetsnivå. En intern kodgranskning, ett automatiserat verktyg eller en revision enligt mall skapar en känsla av trygghet, men den är inte alltid förankrad i verkligheten. Vi hör ofta: "Vi gjorde en egen granskning nyligen – det såg bra ut." Ändå har vi vid första externa testet hittat allvarliga sårbarheter, som RCE (Remote Code Execution) eller exponerad känslig data.

Vi rekommenderar att man kompletterar sitt interna team med en utomstående cybersäkerhetsexpert, som inte är en del av organisationens processer, och ser på miljön med nya ögon. Det är ofta då man hittar de verkliga riskerna. Och för att säkra perspektivet över tid bör man även rotera mellan olika testare, eftersom även de kan bli hemmablinda.

Tänk på:

- **Kombinera intern granskning med extern validering –** Låt det interna säkerhetsarbetet utmanas och kompletteras. Det ger en mer nyanserad bild av nuläget.
- **Genomför externa penetrationstester regelbundet –** Låt oberoende experter försöka ta sig in i era system. Ett pentest avslöjar ofta sådant som interna team missar.
- **Välj rätt partner –** Alla granskningspartner är inte lika vassa. Se till att ni anlitar experter som förstår er verksamhets behov och risker, och är experter på det de gör.

En extern säkerhetsgranskning ger er även ett kvitto på att er säkerhet är testad i praktiken, vilket hjälper till att stärka förtroendet hos både kunder, investerare och styrelse.



5

Svaga autentiserings- och åtkomstkontroller

Autentisering är det första hindret en angripare måste ta sig förbi. Men om det hindret är lågt, eller saknas, spelar det ingen roll hur stark resten av infrastrukturen är. Vi ser fortfarande konton som delas mellan flera användare, lösenord som skickas i klartext, eller flerfaktorsautentisering (MFA) som bara krävs i vissa system. Ibland används till och med standardlösenord på exponerade tjänster. Allt det här öppnar upp för intrång.

Men det handlar inte bara om vem som får logga in, utan också vad den personen kan göra efteråt. Det är två olika saker, och båda är vanliga problem. Dessa listas i OWASP Top 10. Brister i själva autentiseringen klassas under OWASP A07: Authentication Failures. Brister i behörighetshanteringen, alltså åtkomstkontroller, hamnar istället under A01: Broken Access Control, som är bland de allvarligaste och mest förekommande sårbarheterna vi hittar i våra tester.

Exempel på vad vi ofta ser:

- MFA som är konfigurerat men inte krävs för vissa användare eller endpoints. (A07)
- Applikationer som saknar spärrar mot upprepade inloggningsförsök (t.ex. kontolåsning eller rate limiting), vilket gör automatiserade attacker som credential stuffing och hybrid password spray attacks möjliga. (A07)
- Felaktigt hanterade sessionstokens som inte förnyas korrekt eller loggas i klartext. (A07)
- Användare som kan ändra API-anrop eller URL-parametrar för att komma åt andra användares data – trots att de inte har rätt behörighet. (A01)
- Roller och åtkomster som inte är korrekt avgränsade, vilket gör att en vanlig användare kan få adminbehörighet i vissa delar av systemet. (A01)

Den gemensamma nämnaren är små misstag, ofta orsakade av komplexitet, bristande överblick eller otydliga ansvarsområden. Dessa brister skapar en attackyta som ofta kan utnyttjas länge innan någon ens märker att något är fel och kan leda till fullständig kompromettering.

Vad du kan göra:

- **Implementera en central och standardiserad autentiseringslösning**
  Använd etablerade protokoll som SAML eller OIDC istället för hemmasnickrade lösningar.
- **Granska behörigheter – manuellt**
  Automatiserade verktyg kan sällan avgöra vad som borde vara tillåtet. Gör manuella granskningar av rollstrukturer, API-anrop och åtkomstlogik.
- **Ställ krav på MFA överallt – även internt**
  Och verifiera att det verkligen är aktiverat för alla konton och applikationer.
- **Använd least privilege som grundprincip**
  Tilldela aldrig mer rättigheter än vad som krävs, och se till att det gäller både användare och systemintegrationer.
- **Inför spärrar för brute-force-attacker**
  T.ex. kontolåsning eller CAPTCHA vid upprepade försök.
- **Se till att sessionshanteringen är korrekt konfigurerad**
  Tokens ska vara säkra, tidsbegränsade och inte exponerade.
- **Övervaka autentiseringsflöden**
  Identifiera misstänkta inloggningar eller ovanliga beteenden i realtid.

6

Leverantörskedjan

Du kan ha full kontroll över dina egna system, men det räcker inte om dina leverantörer inte håller samma nivå. I dagens IT-landskap är de flesta miljöer uppbyggda av komponenter från andra: tredjepartsbibliotek, API:er, plugins, molntjänster, SaaS-lösningar. Varje sådan integration är en potentiell väg in. Och dessa attacker har ökat markant på sistone. Enligt 2025 Data Breach Investigations Report (DBIR) har andelen intrång där en tredje part var inblandad dubblats jämfört med förgående år; från 15 % 2024, till 30 % 2025.

När angripare inte kommer in genom huvudingången, letar de efter sidoingångar, och leverantörskedjan är ofta just det. Tredjepartsintegrationer, plugins och externa tjänster får sällan samma säkerhetsgranskning som de interna systemen, trots att de kan ha direkt access till affärskritiska data eller funktioner.

Vanliga missar vi ser är:

Applikationer som använder externa komponenter utan att kontrollera uppdateringar eller ägarskiften

Otydliga säkerhetskrav i avtal - otillräckliga SLAs för patchning/ incident reporting och inga krav på oberoende audit eller regelbundna pentest.

Brist på rutiner för säkerhetskrav i inköpsprocessen – säkerheten antas istället för att verifieras.

OWASP listar denna typ av sårbarhet under A03: Software Supply Chain Failures, som täcker just fall där tillit till kod, komponenter eller processer inte följs upp tillräckligt.

Vad du kan göra:

Ställ krav på leverantörer och tredjepartstjänster

Definiera tydliga minimikrav på säkerhetsnivå, uppdateringspolicy, incidentrapportering och rollbaserad åtkomst.

Granska mjukvaruberoenden regelbundet

Håll koll på vilka komponenter ni använder, och hur de förändras över tid.

Ha separata miljöer och åtkomstkontroller för olika leverantörer

Isolera integrationer så att de inte kan påverka kärnsystem vid kompromettering.

Följ upp med återkommande granskningar och säkerhetsdialoger

Det räcker inte att ställa krav vid onboarding, uppföljning krävs.

Implementera Software Composition Analysis (SCA)

Automatiserade verktyg som varnar för sårbara beroenden och licensrisker i kodbasen.

7

Bristande säkerhetskultur

IT-säkerhet handlar som sagt inte bara om teknik, det handlar också om människor. Och just därför är den mänskliga faktorn en av de mest sårbara punkterna i de flesta organisationer. Det bekräftas även i Verizon DBIR 2025, där 60 % av alla intrång involverade mänskliga misstag på något sätt.

En felaktigt klickad länk, en glömd skärm med öppen information, eller en slarvigt hanterad USB-sticka kan räcka för att inleda en kedjereaktion. Även de mest robusta tekniska lösningarna kan kringgås om användarna inte förstår riskerna eller saknar rätt rutiner.

Men säkerhetskultur uppstår inte av sig själv. Den behöver jobbas på, aktivt och över tid. Det räcker inte med en obligatorisk e-learning en gång om året.

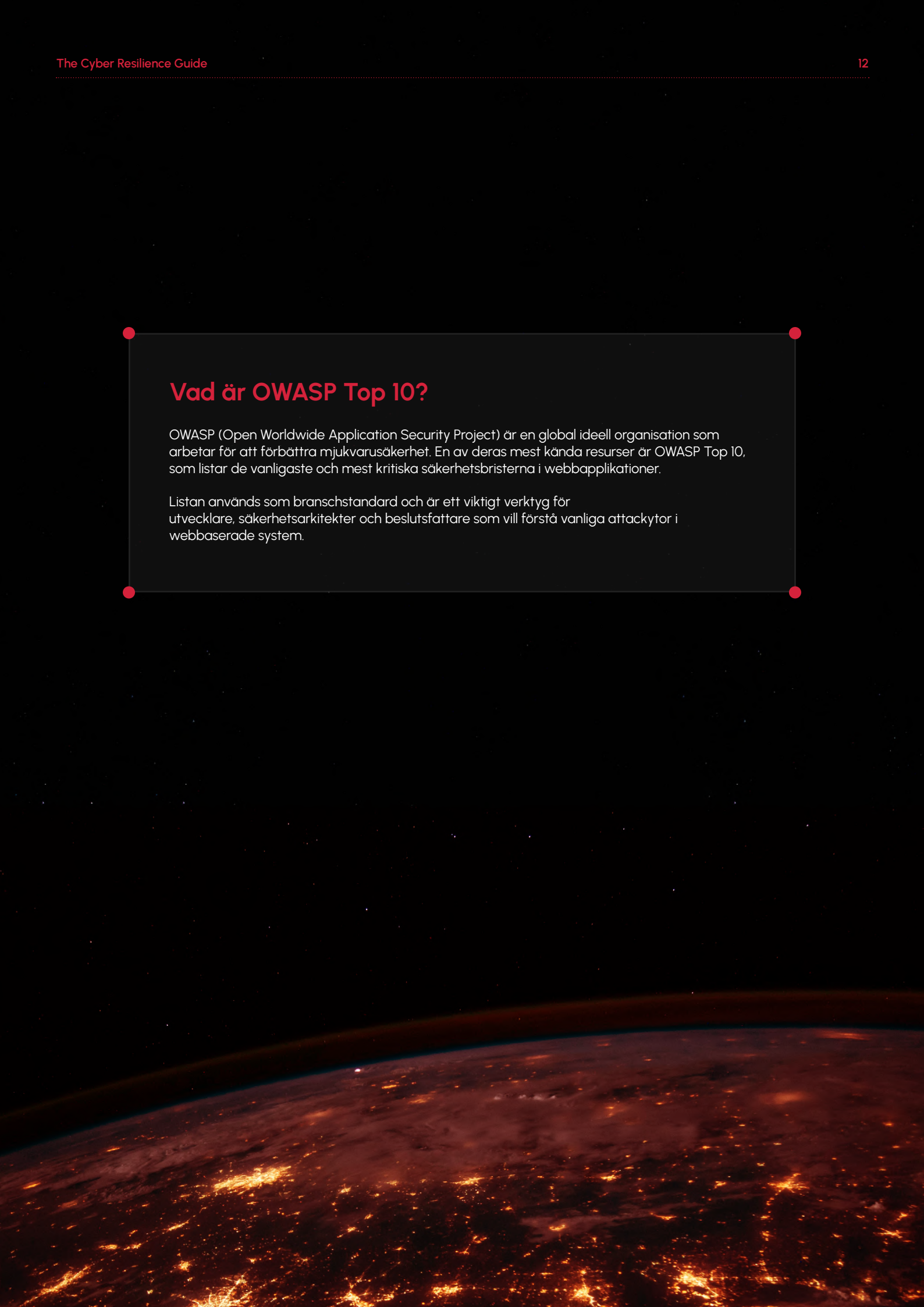
Vad du kan göra:

- **Konfigurera ditt spamfilter**
  Detta för att minimera risken att phishing-mejlet ens når dina anställda.
- **Utbilda kontinuerligt, inte punktvis**
  Skapa ett utbildningsprogram med återkommande insatser, inte bara för IT, utan för hela organisationen. Anpassa innehållet efter roller och risker.
- **Simulera verkliga scenarier**
  Genomför phishing-simuleringar, incidentövningar och rollspel så att alla får öva i realistiska situationer.
- **Sätt säkerhet på agendan**
  Lyft säkerhet i interna nyhetsbrev, avdelningsmöten och onboarding – inte bara i policies.
- **Bygg en kultur där man vågar rapportera**
  Skapa ett klimat där misstänkta händelser rapporteras snabbt, utan skuld eller skam.
- **Följ upp och förbättra**
  Mät säkerhetsbeteenden, samla in feedback och iterera på insatserna. En stark säkerhetskultur är inget man blir klar med.

Vad är OWASP Top 10?

OWASP (Open Worldwide Application Security Project) är en global ideell organisation som arbetar för att förbättra mjukvarusäkerhet. En av deras mest kända resurser är OWASP Top 10, som listar de vanligaste och mest kritiska säkerhetsbristerna i webbapplikationer.

Listan används som branschstandard och är ett viktigt verktyg för utvecklare, säkerhetsarkitekter och beslutsfattare som vill förstå vanliga attackytor i webbaserade system.



Om Cyloq

Vi har arbetat med allt från techbolag och myndigheter till internationella koncerner och kritisk infrastruktur. Med över 15 års erfarenhet i ryggen har vi byggt upp ett sjätte sinne för hur angrepp sker, hur svagheter smyger sig in och var de verkliga riskerna gömmer sig. Och med erfarenhet från både offensiv och defensiv säkerhet vet vi hur angripare tänker, hur försvar faller, och hur de kan förstärkas.

Vi är en partner du kan lita på, med erfarenheten att förstå din verklighet och anpassa vårt arbete efter de specifika krav din bransch ställer.

Redo att se om dina system är så säkra som du tror?

Nu vet du vilka misstag som kan fälla även de mest erfarna säkerhetsteamen. Kunskap räcker långt, men du behöver också testa dina system på riktigt.

Ett penetrationstest är det mest konkreta du kan göra för att hitta brister innan någon annan gör det. Det är en mindre insats som visar exakt var det brister och var ni bör förstärka.

För organisationer med komplexa system, många integrationer och höga säkerhetskrav är en extern granskning det bästa ni kan göra för att garantera att ett system eller applikation faktiskt håller tätt.

Cyloq genomför avancerade, manuella tester med angriparperspektiv. Vi kartlägger attackytan, identifierar sårbarheter och visar exakt hur långt en angripare skulle kunna ta sig, och vad du kan göra för att stoppa det.

Vårt fokus är inte att bekräfta att allt ser bra ut. Vårt fokus är att hitta det som kan sänka dig, innan någon annan gör det. Och om inte vi hittar några luckor, kan du vara säker på att ingen annan gör det heller.

"Vi vill ju att de ska hitta saker, men man har ju också gott självförtroende. Vi tänkte att de inte skulle lyckas med detta på så kort tid."

- Tim, VX Fiber

"Vi blev positivt överraskade. De hittade en hel del som inte hade kommit fram i tidigare penetrationstest eller vårt bug bounty program. Så vi var väldigt nöjda med resultatet penetrationstestet gav!"

- Marcus, Stravito

Förebygg bristerna. Testa på riktigt.

Så här går ett penetrationstest med Cyloq till:

Uppstartsmöte

Vi sätter scopet och målen tillsammans.

Attackfas

Vi angriper din miljö, granskar varje yta, varje länk och varje väg in.

Löpande rapportering

Kritiska brister rapporteras direkt.

Leverans

Du får en konkret rapport med tydliga rekommendationer.

Andreas Gjelset

Cybersecurity Consultant
Tel: +46766777766
Mail: andreas@cyloq.se

Cyloq AB
Pyramidvägen 7, 169 56 Solna
+46 (0) 10 333 10 33
hello@cyloq.se