WHITEPAPER · NOVEMBER 2026

DEDIKO
YOUR SECURITY
OUR PASSION



DETECTION & RESPONSE · NIS2 · LEDELSESANSVAR

Når et login er nok.

Hvorfor klassisk overvågning ikke længere slår til og hvad ledelsen bør kræve af sin sikkerhedsleverandør i 2026.

WHITEPAPER

Indhold

01	Angriberne bryder ikke ind. De logger ind.	03
02	Tre angrebsveje. Standard-MDR ser kun den ene.	04
03	Sikkerhed er blevet et ledelsesansvar	05
04	Byg selv, køb MDR eller saml det hele?	06
05	Fra signal til handling på fire trin	07
06	15 spørgsmål til jeres sikkerhedsleverandør	08
07	Kundecase: tre leverandører samlet til én	09
08	En nordisk specialist i cybersikkerhed	10

RESUMÉ FOR LEDELSEN

Kort fortalt

De fleste alvorlige brud starter ikke med avanceret hacking. De starter med et login, der allerede er lækket, eller en kendt sårbarhed i et system, som vender ud mod internettet. Angriberen logger ind som en almindelig bruger, og derfor opdager klassiske sikkerhedsværktøjer det for sent.

Samtidig er ansvaret rykket op i organisationen. Med NIS2 hæfter ledelsen personligt for, at sikkerheden er tilstrækkelig, og alvorlige hændelser skal varsles inden for 24 timer.

Whitepaperens hovedpointer

- ✓ Standard-MDR reagerer på angreb i gang, men ser ikke lækkede logins og eksponerede sårbarheder.
- ✓ Overvågning, angrebsflade og dark web bør ses samlet. Ellers opstår der huller mellem leverandørerne.
- ✓ Et internt 24/7-SOC er urealistisk for de fleste. Valget står mellem leverandører, og kravene til dem bør være skarpe.
- ✓ Brug de 15 spørgsmål i kapitel 06 til at vurdere jeres nuværende eller kommende leverandør.

Angriberne bryder ikke ind. De logger ind.

For ti år siden handlede IT-sikkerhed især om at holde angriberne ude: firewalls, antivirus og segmenterede netværk. Den model er ikke forkert, men den rammer ved siden af den måde, de fleste angreb sker på i dag.

Ifølge Verizons Data Breach Investigations Report 2025 starter 22 % af brudene med misbrugte logins, og 20 % starter med udnyttelse af en kendt sårbarhed. Det sidste er steget med en tredjedel på ét år. Samlet set involverer omkring 60 % af bruddene det menneskelige led: phishing, social engineering eller misbrugte adgangskoder. Andre opgørelser når endnu højere: en analyse af de brud, der blev anmeldt til det britiske datatilsyn, fandt, at ni ud af ti skyldtes menneskelige fejl.

Logins bliver typisk stjålet af såkaldt infostealer-malware på medarbejdernes private eller arbejdsrelaterede enheder. De bliver solgt videre på dark web-markeder. Når angriberen så logger ind, ligner det en helt almindelig bruger. Der er ingen malware at opdage og intet mistænkeligt vedhæftet dokument, kun et gyldigt brugernavn og en adgangskode.

Tiden arbejder for angriberen

IBM's Cost of a Data Breach Report 2025 viser, at det i gennemsnit tager 241 dage at opdage og inddæmme et brud. I den periode kan angriberen kortlægge netværket, skaffe sig flere rettigheder, stjæle data og forberede krypteringen. Jo længere angrebet står på, før det bliver opdaget, desto dyrere bliver det.

22 %
af brudene starter med misbrugte logins

20 %
udnytter en kendt sårbarhed (+34 % på ét år)

~90 %
af brud kan spores til menneskelige fejl

241
dage i snit til at opdage og inddæmme et brud

Kilder: Verizon DBIR 2025 · IBM Cost of a Data Breach 2025 · CybSafe / UK ICO

> **Spørgsmålet er ikke, om et login er lækket, men om I opdager det, inden det bliver brugt.**

Tre angrebsveje. Standard-MDR ser kun den ene.

MDR (Managed Detection & Response) er blevet standardsvaret på manglende sikkerhedsressourcer: en ekstern leverandør overvåger jeres miljø døgnet rundt og griber ind, når noget sker. Det er værdifuldt. Men MDR er bygget til at reagere, og det betyder, at angrebet allerede skal være i gang, før tjenesten træder i kraft.

SES AF MDR

Aktive angreb

Mistænkelig adfærd på endpoints, servere, i identiteter og i cloud. MDR opdager og stopper det, **men først når det sker.**

BLIND VINKEL

Lækkede logins

Brugernavne og adgangskoder til salg på dark web. Indtil de bliver brugt, er der intet at opdage i jeres eget miljø.

BLIND VINKEL

Eksponerede sårbarheder

Glemte subdomæner, testservere og upatchede VPN-gateways. Angriberne scanner efter dem automatisk.

Hvorfor det betyder noget

Verizon fandt, at 54 % af ransomware-ofrene havde domæner, der optrådte i infostealer-data, før angrebet skete. Advarslen lå med andre ord fremme, men den blev ikke set, fordi ingen kiggede efter den.

Det samme gælder angrebsfladen. Mange organisationer har ikke et opdateret overblik over, hvad de har eksponeret mod internettet. Det gælder især efter cloud-migreringer, opkøb eller projekter, hvor en leverandør har sat noget op og glemt det igen.

Løsningen er ikke at droppe MDR, men at supplere med **proaktiv overvågning** af de to blinde vinkler: dark web-overvågning og EASM/CTEM. Samlet kaldes det **MxDR**: Managed Extended Detection & Response.

54 %

af ransomware-ofre havde lækkede logins i infostealer-data, før angrebet

2 af 3

angrebsveje er usynlige for en rent reaktiv MDR-tjeneste

Kilde: Verizon DBIR 2025

SÅDAN LUKKER DEDIKO MXDR ALLE TRE

REAKTIV
MDR 24/7
35+ Tier 3-analytikere opdager og inddæmmer aktive angreb døgnet rundt.

PROAKTIV
Dark web-overvågning
Lækkede logins fra jeres domæner findes og spærres, før de bliver brugt.

PROAKTIV
EASM/CTEM
Jeres eksterne angrebsflade kortlægges løbende, så åbne døre lukkes først.

Én kontrakt · én rapport · 30 timers incident response inkluderet Læs mere i kapitel 05 og 08 →

DEDIKO
YOUR SECURITY
OUR PASSION

Sikkerhed er blevet et ledelsesansvar

Med NIS2, der i Danmark er gennemført med NIS2-loven, er cybersikkerhed ikke længere kun et IT-anliggende. Ledelsen i omfattede virksomheder skal godkende og føre tilsyn med sikkerhedsforanstaltningerne og kan holdes personligt ansvarlig, hvis de ikke er tilstrækkelige.

NÅR HÆNDELSEN SKER: NIS2'S FRISTER

24 timer
Varsling

Første varsling til myndighederne om en væsentlig hændelse.

72 timer
Hændelsesrapport

Vurdering af hændelsens alvor, omfang og indikatorer.

1 måned
Endelig rapport

Årsag, konsekvenser og de tiltag, der er sat i værk.

Fristerne forudsætter, at I opdager hændelsen i tide og kan dokumentere forløbet. Det kræver overvågning, der kører døgnet rundt.

MAKSIMALE BØDER

NIS2, væsentlige enheder	**10 mio. € eller 2 % af global omsætning**
NIS2, vigtige enheder	**7 mio. € eller 1,4 % af global omsætning**
GDPR, alle der behandler persondata	**20 mio. € eller 4 % af global omsætning**
DORA, den finansielle sektor	Fastsættes nationalt af tilsynet

Også uden for NIS2

GDPR gælder alle, der behandler persondata. Den største regning er dog ofte driftsstoppet: en lukket webshop, en standset produktion og kunder, der går til konkurrenten.

For ledelsen er spørgsmålet ikke længere teknisk. Det handler om at kunne dokumentere, at man har handlet ansvarligt.

Kilder: NIS2 (EU) 2022/2555 · DORA (EU) 2022/2554 · GDPR (EU) 2016/679. Bøder: det højeste af de to beløb. Ikke juridisk rådgivning.

Byg selv, køb MDR eller saml det hele?

Døgnovervågning kræver mennesker, der er vågne. En enkelt bemandet plads 24/7 året rundt kræver typisk fem til seks fuldtidsansatte, når man regner med ferie, sygdom og vagtplaner. Dertil kommer licenser til SIEM og EDR, threat intelligence, efteruddannelse og en ledelse, der kan fastholde specialister på et marked med stor mangel på dem. For de fleste danske virksomheder er et internt SOC derfor ikke realistisk. Valget står mellem eksterne modeller.

MODEL A

Internt SOC

Fuld kontrol og dybt kendskab til forretningen.

- Kræver 5-6 FTE pr. bemandet plads
- Svært at rekruttere og fastholde
- Høj fast omkostning

MODEL B

Standard-MDR

24/7-overvågning og respons som abonnement.

- Reagerer først, når angrebet er i gang
- Dark web og angrebsflade købes ofte separat
- Incident response ofte på timepris

MODEL C

Samlet MxDR

MDR + dark web + EASM/CTEM i én leverance.

- ✓ Dækning før, under og efter angrebet
- ✓ Én kontrakt og én rapport
- ✓ 30 timers incident response inkluderet

Skjulte omkostninger ved flere leverandører

Mange organisationer ender med tre til fire separate aftaler: én til MDR, én til sårbarhedsscanning, én til dark web-overvågning og en rammeaftale om incident response til timepris. Hver aftale kan give mening for sig, men tilsammen giver de tre problemer: hullerne mellem leverandørerne, et fragmenteret overblik for ledelsen og en samlet pris, som sjældent bliver gjort op.

Sammenlign derfor ikke kun månedsprisen på MDR. Gør den samlede årlige omkostning op, inklusive onboarding og den forventede pris på incident response, hvis uheldet er ude.

5-6

fuldtidsansatte til én bemandet plads døgnet rundt*

1,9 mio. $

lavere omkostning pr. brud ved udstrakt brug af AI og automatisering

*Tommelfingerregel for skiftedrift. Kilde: IBM Cost of a Data Breach 2025

DEDIKO
YOUR SECURITY OUR PASSION

Fra signal til handling på fire trin

En samlet detektionsmodel består af data fra hele miljøet, intelligens udefra, automatiseret sortering og mennesker, der træffer beslutningen. Det afgørende er ikke antallet af alarmer, men hvor hurtigt en reel trussel bliver bekræftet og stoppet.

1

Indsamle

Data fra endpoints, servere, identiteter, cloud, e-mail og netværk samles ét sted.

2

Berige

Hændelser bliver krydstjekket med dark web-fund, angrebsfladen og threat intelligence.

3

Vurdere

AI sorterer støjen fra. En specialist validerer de alarmer, der er tilbage.

4

Handle

Konto spærres, enhed isoleres, og kunden får besked med det samme.

EKSEMPEL PÅ EN ALARM

● KRITISK risikoscore 94/100

Kompromitteret brugerkonto

Login fra kendt Tor-exit-node. Brugerens adgangskode er fundet i infostealer-data på dark web. Mønsteret matcher MITRE ATT&CK T1078 (Valid Accounts).

Respons: kontoen er deaktiveret, sessioner er afbrudt, og kunden har fået besked.

Datakilder: fra 5 til 11

En standard-MDR ser typisk fem kilder. En samlet model tilføjer de proaktive kilder:

Identitet · Netværk · Cloud & SaaS · Endpoint · E-mail

Dark web · Canary tokens · EASM/CTEM · AD-review · EDR/XDR-review · Incident response

DEDIKO MXDR

Minutter

fra kritisk alarm til inddæmning. Automatisk alarmhåndtering og validering af en specialist.

BRANCHETAL · IBM 2025

Organisationer med udstrakt brug af AI og automatisering har i gennemsnit **80 dage kortere** brudforløb og **1,9 mio. $ lavere** omkostninger pr. brud end organisationer uden.

Hvorfor mennesket stadig er afgørende

AI er god til at sortere tusindvis af hændelser og finde mønstre. Men beslutningen om at spærre en direktørs konto midt i et kundemøde eller isolere en produktionsserver kræver kontekst og dømmekraft. Kræv derfor, at en specialist validerer alle kritiske alarmer.

Hvad ledelsen bør se hver måned

Antal hændelser og hvordan de blev håndteret, nye fund på dark web og i angrebsfladen, svartider målt mod SLA og hvilke anbefalinger der er åbne. Ikke tekniske logs, men et billede af risikoen.

Alarmen er et illustrativt eksempel. Branchetal: IBM Cost of a Data Breach 2025, gennemsnit på tværs af organisationer, ikke Dedikos svartider.

DEDIKO
YOUR SECURITY
OUR PASSION

15 spørgsmål til jeres sikkerhedsleverandør

Brug spørgsmålene til at vurdere jeres nuværende leverandør eller til at sammenligne tilbud. Et godt svar er konkret, målbart og står i kontrakten.

Dækning

01 Hvilke datakilder overvåger I, og hvilke ligger uden for aftalen? Firewall? On-prem?

02 Overvåger I dark web for lækkede logins fra vores domæner?

03 Kortlægger I løbende vores eksterne angrebsflade? EASM/CTEM

04 Er der en menneskelig analytiker på vagt hele døgnet, også i weekender og på helligdage?

Respons

05 Må I handle selv, fx isolere en enhed eller spærre en konto, eller sender I kun en alarm?

06 Hvilke SLA'er har I på opdagelse (MTTD) og respons (MTTR), og hvordan måles de?

07 Er incident response og forensics inkluderet, og hvor mange timer?

08 Kan I hjælpe os med at overholde fristen på 24 timer for varsling efter NIS2?

Mennesker og teknologi

09 Hvilket kompetenceniveau har analytikerne, og hvor sidder de?

10 Hvordan bruger I AI, og hvor træffer et menneske next step beslutningen?

11 Kan I arbejde med vores eksisterende værktøjer (fx Defender, Cortex, SentinelOne)?

Rapportering og økonomi

12 Hvad indeholder rapporten til ledelse og bestyrelse, og hvor ofte kommer den?

13 Hvor opbevares vores data, og er det i overensstemmelse med GDPR?

14 Hvad koster onboarding, og hvor lang tid tager det?

15 Hvad er den samlede årlige pris inklusive alle tillæg?

Kundecase: tre leverandører samlet til én

⚠ KUNDECASE Priserne nedenfor stammer fra én konkret, anonymiseret kunde og afspejler kundens miljø, antal brugere og valgte services. De er **ikke en listepris**. Jeres pris afhænger af jeres miljø og beregnes individuelt.

UDGANGSPUNKT

Kunden havde MDR hos én leverandør, sårbarhedsscanning og dark web-overvågning hos andre og incident response til timepris på 1.700-3.400 kr.

LØSNING

Alt blev samlet i Dediko MxDR med EASM/CTEM, dark web-overvågning, 30 timers incident response, kvartalsvis EDR/XDR-review og Entra AD-review inkluderet.

RESULTAT

Flere datakilder overvåges (fra 5 til 11), der er én kontrakt og én månedlig rapport, og omkostningen det første år faldt med 51 %.

FØR: TIDLIGERE LEVERANDØR	PR. MD.
MDR	**17.500,-**
Incident response (ingen timer inkl.)	**5.000,-**
Sårbarhedsscanning (uden EASM)	**8.000,-**
Dark web-overvågning	**3.000,-**
Onboarding (engangsbeløb, gns.)	**15.000,-**
Total første år	**417.000,-**

EFTER: DEDIKO MXDR	PR. MD.
MxDR, alle services inkluderet	**17.000,-**
Incident response (30 timer inkl.)	**Inkluderet**
EASM/CTEM-scanning	**Inkluderet**
Dark web-overvågning	**Inkluderet**
Onboarding	**Inkluderet**
Kvartalsvis EDR/XDR-review	**Inkluderet**
Entra AD-review (ved onboarding)	**Inkluderet**
Total første år	**204.000,-**

I DENNE CASE **213.000,- sparet første år** 51 % lavere pris for mere dækning

HVAD KAN ANDRE LÆRE AF CASEN?

- ✓ Gør den samlede årlige pris op, ikke kun MDR-linjen.
- ✓ Incident response på timepris er en ukendt regning, indtil det går galt.
- ✓ Flere leverandører betyder ikke mere sikkerhed, men flere huller imellem.

Kundecase: priser i DKK ekskl. moms pr. måned for én konkret kunde. Onboarding er engangsbeløb. Scanning og dark web var rabatpriser hos den tidligere leverandør.

DEDIKO
YOUR SECURITY
OUR PASSION

En nordisk specialist i cybersikkerhed

Dediko A/S har rødder tilbage til 1995, hvor Draware blev grundlagt som driftsselskab inden for cybersikkerhed. Aktiviteterne var en del af Deloitte Risk Advisory fra 2020, blev udskilt som Dediko A/S i 2022 og har siden 2025 været en del af den nordiske koncern HAWK Infinity.

Sammen med vores partnere leverer vi hele kæden: rådgivning og compliance, offensive tests, 24/7 detection & response og træning. Det betyder én partner og én stack, fra den første risikovurdering til responsen den nat, det går galt.

Vi holder prisen nede ved at bruge et SOC med mere end 35 Tier 3-analytikere i Polen og drive vores datacenter på Island med næsten 100 % vedvarende energi og gratis køling året rundt.

400+
kunder i Norden

35+
Tier 3-analytikere i SOC'en

35+
teknologipartnere

24/7
overvågning og respons

Rådgivning & compliance

- vCISO og vDPO
- NIS2 · DORA · ISO 27001
- CIS-analyse
- BCP/DR & tabletop

Offensiv sikkerhed

- Pentest (app, cloud)
- Red & purple teaming
- Phishing-test
- M365 & AD hardening

Detection & response

- **MxDR**
- Dark web & EASM/CTEM
- Honeypots
- IR & forensics

Træning

- Awareness
- Ledelse & bestyrelse
- NIS2 & GDPR
- Secure development

Næste skridt: en uforpligtende gennemgang

Vi gennemgår jeres nuværende setup med de 15 spørgsmål fra kapitel 06 og viser, hvor hullerne er.

SCAN QR-KODEN →

Dediko A/S · Herstedvang 14
2620 Albertslund
+45 45 76 20 21
info@dediko.dk

Referencer

1. Verizon (2025): Data Breach Investigations Report 2025.
2. IBM Security / Ponemon Institute (2025): Cost of a Data Breach Report 2025.
3. Europa-Parlamentets og Rådets direktiv (EU) 2022/2555 (NIS2) og den danske NIS2-lov.
4. Forordning (EU) 2022/2554 om digital operationel modstandsdygtighed i den finansielle sektor (DORA).
5. Forordning (EU) 2016/679 (GDPR), artikel 83.
6. CybSafe: analyse af databrud anmeldt til UK Information Commissioner's Office (ICO), data fra 2019.

Om denne whitepaper

Dokumentet er udarbejdet af Dediko A/S som generel information og er ikke juridisk rådgivning. Bødeniveauer og frister er gengivet i forenklet form. Vurder altid jeres konkrete forpligtelser med en juridisk rådgiver. Priser i kundecasen gælder én konkret, anonymiseret kunde og er ikke et tilbud.

© 2026 Dediko A/S · CVR 18663295
dediko.dk