TDC Erhverv

TDC Erhverv Sikkerhedsrapport Q2 2026

Q2, kort fortalt

Q2 2026 viser et trusselsbillede, hvor velkendte cybertrusler fortsat udvikler sig og finder nye angrebsveje. I løbet af kvartalet observerede TDC Erhverv Cyber Threat Intelligence **1.343** hændelser i internettrafikken, der indikerer kompromittering med malware blandt virksomheder og organisationer i Danmark.

Rapporten peger særligt på tre udviklinger inden for cybertrusler i Danmark:

- Mirai-malwaren – en gammel kending – er tilbage som en markant aktør i trusselsbilledet. Mirai stod for 24,9 % af de observerede hændelser i Q2 2026 og er blandt de mest udbredte malwarekampagner i kvartalet.
- Virksomheder inden for computerprogrammering, it-infrastruktur og it-konsulentbistand var hårdest ramt i Q2 og stod for hele 17,3 % af de observerede hændelser. Det understreger, hvordan virksomheder med høj digital eksponering og adgang til kunders systemer fortsat udgør attraktive mål for ondsindede aktører.
- TDC Erhverv Cyber Threat Intelligence observerede omfattende scanninger rettet mod VPN-løsninger hos danske virksomheder og organisationer. Observationerne viser, hvordan aktører hurtigt omsætter offentlig viden om nye sårbarheder til operationel aktivitet – og hvordan trusselsdata kan anvendes til at prioritere sikkerhedsindsatsen.

På tværs af rapportens analyser står én ting klart: Cybertrusler handler ikke kun om selve angrebet, men i stigende grad om forberedelsen til det. Kortlægning af sårbare systemer, kompromittering af internetforbundne enheder og udnyttelse af nye sårbarheder sker ofte længe før det egentlige angreb. Derfor bliver evnen til at omsætte trusselsindsigter til handling stadig vigtigere for virksomheder og organisationer i Danmark.

Datagrundlaget bag rapporten

I TDC Erhverv leverer vi internettrafik til små, mellemstore og store virksomheder samt myndigheder og offentlige institutioner i Danmark. Det giver os adgang til unik metadata, som vi analyserer i realtid og omsætter til et repræsentativt overblik over det aktuelle trusselsbillede på tværs af bl.a. brancher, virksomhedstyper og geografiske områder[1].

Metadataen bygger på mere end 100 milliarder anonymiserede flowdatapunkter for den trafik, der passerer gennem vores netværk fra og til kunderne. Et flowdatapunkt er et registreret stykke metadata om netværkstrafik – altså information om, at en digital forbindelse har fundet sted, uden indsigt i selve indholdet. Det kan for eksempel være oplysninger om, hvilke enheder der kommunikerer, hvornår kommunikationen sker, hvor længe den varer, og hvilke protokoller eller tjenester der bruges.

Et flow i netværkstrafik kan altså forstås som en "samtale" mellem to enheder. Det beskriver en gruppe datapakker, der hører sammen, fordi de har samme kilde, destination, porte og protokol. For eksempel vil en computers eller smartphones hentning af en hjemmeside fra en server blive registreret som ét flow. Alt dette sammenholdes og analyseres i enorm skala med kunstig intelligens og avancerede analyser – bl.a. ved hjælp af Danmarks nationale AI-supercomputer Gefion. Resultatet er dansk trusselsindsigt, som giver os og vores kunder et unikt forspring i arbejdet mod cyberangreb.

[1] Datagrundlaget er analyseret ud fra gældende indikatorer på tidspunktet for udarbejdelsen. Resultaterne er derfor med forbehold for ændringer, hvis ny information eller nye efterretninger fremkommer.

Q2 2026 i tal

1.343

Hændelser blandt virksomheder og organisationer i Danmark, der indikerer kompromittering med malware i Q2 2026.

I Q2 2026 observerede TDC Erhverv Cyber Threat Intelligence 1.343 hændelser i internettrafikken, der indikerer, at de berørte virksomheder sandsynligvis har været kompromitteret med malware. Som nævnt i TDC Erhverv Sikkerhedsrapport Q1 2026, kan ét vellykket angreb være nok til at skabe store driftsmæssige og økonomiske konsekvenser – med vurderede omkostninger på op til 500.000 kr. per dag for store virksomheder i tilfælde af nedlukning af systemer som følge af et vellykket cyberangreb.

Derfor er det vigtigt at holde et vågent øje med digitale trusler. Vi har i dette kvartal, foruden cryptominere og spambotten Tofsee, observeret en stor mængde hændelser relateret til malwarefamilierne XWorm – en Remote Access Trojan, der giver aktørerne mulighed for at få fjernadgang til kompromitterede enheder – og Mirai, som primært er kendt for at kompromittere internetforbundne enheder og anvende dem i større botnet- og DDoS-angreb.

Mirai er særlig interessant, da truslen har eksisteret i mange år og i en længere periode har fyldt relativt lidt i trusselsbilledet. I dette kvartal har vi imidlertid set en markant stigning i aktiviteten. Hele 24,9 % af de registrerede hændelser i Q2 2026 var relateret til Mirai – en udvikling, vi dykker dybere ned i senere i rapporten.

Top 3 mest udbredte malwarekampagner*

1. XWorm, 25 %
2. Mirai, 24,9 %
3. VShell, 12 %

Top 3 mest udsatte/angrebne brancher

1. Computerprogrammering, it-infrastruktur og it-konsulentbistand: 17,3 %
2. Detailhandel: 12,8 %
3. Engroshandel: 7,3 %

Observerede hændelser efter virksomhedsstørrelse:

1. 1-100 ansatte: 45,1%
2. 100-1000: 23,3%
3. 1000+: 31,5%

* Toplisten omfatter malwarekampagner, der kan klassificeres entydigt på tværs af vores datagrundlag. Derudover observerede vi et højt aktivitetsniveau relateret til blandt andet Tofsee-malware og forskellige typer cryptominere, som også har været en del af det samlede trusselsbillede i Q2 2026.

Mirai – malwaren der gør comeback

Mirai var blandt de mest observerede malwarefamilier i Q2 2026 og adskiller sig fra billedet i Q1, hvor aktiviteten var langt mindre fremtrædende. I alt var 24,9 % af de registrerede hændelser i kvartalet relateret til Mirai, hvilket gør det til en af de mest markante observationer i TDC Erhverv Cyber Threat Intelligence's datagrundlag.

Samtidig blev Mirai-relaterede hændelser observeret på tværs af både sektorer og virksomhedsstørrelser. Det peger på en aktivitet, der ikke er begrænset til enkelte brancher, men som rammer bredt på tværs af det danske trusselsbillede – og en aktivitet, som vi bør tage alvorligt.

Hvad er Mirai?

Mirai er en malwarefamilie, der primært er udviklet til at kompromittere internetforbundne enheder og bruge dem i såkaldte botnets. Et botnet består af kompromitterede enheder, som kan fjernstyres af en operatør og bruges til blandt andet at gennemføre distribuerede overbelastningsangreb (DDoS), hvor store mængder trafik sendes mod en hjemmeside, applikation eller digital tjeneste med det formål at overbelaste den og gøre den helt eller delvist utilgængelig for brugere.

Malwaren er særligt kendt for at målrette Internet of Things-enheder (IoT), såsom IP-overvågningskameraer, smart-tv'er, Android-baserede mediebokse, routere og andet netværksudstyr. Disse enheder har ofte begrænset sikkerhed, sjældne opdateringer og bliver i mange tilfælde sat op uden ændring af standardkonfigurationer, hvilket gør dem attraktive mål for automatiserede angreb.

Mirai blev første gang kendt i 2016, men malwarefamilien fortsætter med at udvikle sig. En væsentlig årsag er, at kildekoden blev offentliggjort for flere år siden, hvilket har gjort det muligt for forskellige aktører at udvikle egne versioner og tilpasse angrebene til nye teknologier og sårbarheder. Samtidig vokser antallet af internetforbundne enheder fortsat, og mange IoT-enheder er utilstrækkeligt sikrede, eksempelvis fordi de anvender standardadgangskoder, mangler sikkerhedsopdateringer eller er eksponeret direkte mod internettet. Derfor ser vi fortsat Mirai-baseret aktivitet år efter år.

"Mange IoT-enheder er utilstrækkeligt sikrede, eksempelvis fordi de anvender standardadgangskoder, mangler sikkerhedsopdateringer eller er eksponeret direkte mod internettet."

Aktivitet rettet mod Android-enheder

Selvom Mirai traditionelt forbindes med kompromittering af IoT-enheder som kameraer, routere og andet netværksudstyr, relaterede en stor del af de observerede hændelser i Q2 2026 sig til aktivitet rettet mod Android-baserede enheder. Konkret observerede TDC Erhverv Cyber Threat Intelligence et meget stort antal forbindelser mod TCP-port 5555 på tværs af et stort antal IP-adresser.

TCP-port 5555 anvendes af Android Debug Bridge (ADB), et værktøj, der bruges til udvikling, administration og fejlfinding af Android-enheder. Hvis ADB efterlades åbent mod internettet, kan ondsindede aktører i nogle tilfælde få mulighed for at få adgang til enheden på afstand, udføre kommandoer og installere skadelig kode. Det kan eksempelvis ske, hvis en Android-baseret enhed såsom et smart-tv, en medieboks eller andet netværksforbundet udstyr er sat op, så administrationsfunktionen kan tilgås direkte fra internettet i stedet for kun fra organisationens interne netværk.

De observerede hændelser indikerer sandsynlige forsøg på at identificere og kompromittere interneteksponerede Android-enheder med ADB aktiveret. På baggrund af den observerede aktivitet vurderer vi, at formålet sandsynligvis er at indrullere enhederne i et Mirai-baseret botnet, hvor de efterfølgende kan bruges som en del af større DDoS-angreb.

Observationerne stemmer overens med en kampagne beskrevet af sikkerhedsforskere fra Hunt.io, som i foråret 2026 identificerede et Mirai-baseret botnet under navnet xlabs_v1. Kampagnen var specifikt rettet mod Android-enheder med eksponeret ADB på TCP-port 5555 og havde til formål at opbygge et botnet til brug for såkaldte DDoS-for-hire-angreb. Her kan aktører købe eller leje adgang til et eksisterende botnet og bruge de kompromitterede enheder til at gennemføre DDoS-angreb mod udvalgte mål.

Hvorfor er Mirai stadig farlig?

Mirai er et godt eksempel på, at ældre malwarefamilier fortsat kan udgøre en betydelig trussel, selv mange år

efter deres oprindelige fremkomst. Hvor nutidens cybertrusler ofte forbindes med ransomware, AI eller avancerede spionageoperationer, viser Mirai, at relativt velkendte værktøjer stadig kan have stor effekt, når de kombineres med dårligt sikrede internetforbundne enheder, fx IoT-enheder, der ofte ikke modtager samme sikkerhedsmæssige opmærksomhed som traditionelle computere og servere.

Når sådanne enheder kompromitteres i stort antal, kan de bruges som byggesten i omfattende botnets med kapacitet til at gennemføre store DDoS-angreb mod virksomheder, organisationer, offentlige institutioner og samfundskritiske anlæg som fx el- og vandværker.

Aktiviteten i Q2 2026 understreger altså vigtigheden af løbende at have overblik over interneteksponerede enheder, der anvendes til drift, overvågning eller daglige arbejdsopgaver, som ofte er overset i den daglige drift.

"Når IoT-enheder kompromitteres i stort antal, kan de bruges som byggesten i omfattende botnets med kapacitet til at gennemføre store DDoS-angreb mod virksomheder, organisationer, offentlige institutioner og samfundskritiske anlæg som fx el- og vandværker."

It-branchen er den mest ramte sektor i Q2 2026

17,3 % af de observerede hændelser i Q2 2026 relaterede sig til virksomheder inden for computerprogrammering, it-infrastruktur og it-konsulentbistand. Dermed er it-branchen den mest ramte sektor i kvartalet – og en sektor, der kan have store konsekvenser for andre brancher.

It-branchen ligger ofte højt i TDC Erhverv Cyber Threat Intelligences observationer. Det skyldes sandsynligvis branchens høje grad af digital eksponering. Virksomheder inden for softwareudvikling, drift, hosting, cloud, infrastruktur og konsulentydelser arbejder typisk med et stort antal internetvendte systemer, udviklingsmiljøer, API'er og fjernadgange. Samtidig er mange it-miljøer komplekse og under konstant udvikling, hvilket kan gøre det vanskeligt løbende at identificere og lukke alle potentielle angrebsflader.

"Jo flere systemer der er eksponeret mod internettet, desto flere muligheder har ondsindede aktører for at identificere sårbarheder, fejlkonfigurationer eller kompromitterede legitimationsoplysninger, der kan bruges til at opnå adgang."

Når én virksomhed kan åbne døren til mange andre

It-virksomheder adskiller sig samtidig fra mange andre brancher ved, at de ofte har privilegeret adgang til kunders systemer, netværk og data. Det kan for eksempel være gennem driftsovervågning, supportfunktioner, cloud-platforme, integrationsløsninger eller administrative værktøjer. Hvis en it-leverandør kompromitteres, kan det altså i nogle tilfælde give aktørerne mulighed for at bevæge sig videre mod de virksomheder, der er kunder hos it-leverandørerne.

Derfor kan konsekvenserne af et vellykket sikkerhedsbrud række langt ud over den enkelte virksomhed. It-virksomheder kan fungere som et attraktivt springbræt til flere organisationer samtidigt, hvilket gør sektoren interessant for aktørerne.

Malwarefamilierne fortæller en vigtig historie

De observerede hændelser for Q2 2026 relaterede sig blandt andet til malwarefamilierne Mirai, XWorm, VShell og RisePro – sidstnævnte beskrevet i dybden i forrige udgivelse af TDC Erhverv Sikkerhedsrapport. Fælles for disse er, at de indgår i et trusselsbillede præget af bredt distribuerede malwarekampagner og kompromitteringsforsøg, og er bredt brugt blandt aktører. RisePro er eksempelvis en såkaldt infostealer, der er designet til at stjæle loginoplysninger, browserdata og anden følsom information, mens XWorm giver aktører mulighed for at fjernstyre kompromitterede systemer.

Sammensætningen af malwarefamilierne tyder på, at en stor del af aktiviteten er opportunistisk. Frem for målrettede kampagner mod specifikke virksomheder ser vi tegn på aktører, der i stor skala scanner efter kendte sårbarheder, svage adgangskoder, fejlkonfigurationer eller andre muligheder for kompromittering. Det viser, at selv relativt velkendte trusler fortsat kan skabe risici, hvis grundlæggende sikkerhedsforanstaltninger ikke er på plads.

Hvad betyder det for it-branchen?

Observationerne fra Q2 2026 viser, at it-virksomheder fortsat er attraktive mål i trusselsbilledet. Ikke nødvendigvis fordi de ligger inde med de mest værdifulde data, men fordi de ofte har adgang til deres kunders systemer, infrastruktur og informationer. Kunderne kan blandt andet omfatte virksomheder i den private sektor, offentlige myndigheder, kommuner og organisationer med samfundsvigtige funktioner.

For it-virksomheder betyder det, at løbende overvågning, patch management og styring af privilegerede adgange er særligt vigtigt. Jo hurtigere kompromitteringsforsøg opdages, desto mindre er sandsynligheden for, at de udvikler sig til egentlige sikkerhedshændelser.

Hvad betyder det for virksomheder, der benytter it-leverandører?

For de fleste virksomheder er it-leverandører efterhånden en integreret del af den daglige drift. Det kan være i forbindelse med alt fra hosting- og cloudleverandører til udviklingshuse, driftspartnere eller virksomheder, der leverer it-support og administration.

Det betyder, at stærk cybersikkerhed ikke længere kun handler om egne systemer, men også om sikkerheden hos de leverandører og samarbejdspartnere, man giver adgang til sine data og sin infrastruktur.

Når virksomheder køber og anvender eksterne it-services, kan det derfor være relevant at skabe overblik over:

- Hvilke systemer og data leverandøren får adgang til
- Om adgangen er begrænset til kun det nødvendige
- Hvordan leverandøren overvåger sikkerhedshændelser og kompromitteringsforsøg
- Leverandørens protokol for opdateringer, adgangsstyring og multifaktorgodkendelse
- Hvordan sikkerhedshændelser håndteres, hvis leverandøren bliver kompromitteret

Jo større indsigt virksomheder har i deres digitale afhængigheder, desto bedre forudsætninger har de for at reducere risikoen for, at et angreb hos leverandøren udvikler sig til et problem for virksomheden.

Kan Cyber Threat Intelligence forudsige morgendagens angreb?

I Q2 2026 observerede TDC Erhverv Cyber Threat Intelligence omfattende sårbarheds-scanninger rettet mod danske virksomheder og organisationer. Observationerne rejser et interessant spørgsmål: Kan Cyber Threat Intelligence-data bruges som en tidlig indikator for, hvilke sårbarheder angriberne prioriterer, og dermed hvilke angreb der kan være på vej?

Sårbarheden CVE-2026-0257 fik øget opmærksomhed, efter der blev offentliggjort et såkaldt proof-of-concept (PoC) – kode, der demonstrerer, hvordan en sårbarhed kan udnyttes, og som ofte anvendes af sikkerhedsforskere til dokumentation og analyse. Når sådan kode bliver offentlig tilgængelig, kan den imidlertid også anvendes af ondsindede aktører til hurtigt at udvikle eller automatisere angreb. Efter offentliggørelsen har TDC Erhverv Cyber Threat Intelligence observeret scanninger rettet mod mere end 1.000 danske virksomheder og organisationer og 400 af disse inden for blot de første timer.

Derudover observeredes aktivitet relateret til CVE-2026-50751, som ligeledes er blevet udnyttet af trussels-aktører i forbindelse med kompromitteringsforsøg. Fælles for begge sårbarheder er, at de påvirker VPN-løsninger, som ofte har en central placering i organisationers netværksarkitektur.

Begge sårbarheder er såkaldte authentication bypass-sårbarheder relateret til VPN-løsninger. Det betyder, at en angriber under bestemte omstændigheder kan omgå de normale loginmekanismer og opnå adgang til systemet uden at gennemføre den forventede autentificering. Hvis en sådan sårbarhed udnyttes, kan den potentielt give adgang til interne ressourcer, som ellers kun skulle være tilgængelige for autoriserede brugere.

For angribere er sårbarheder generelt interessante, fordi de kan fungere som en genvej ind i organisationers it-miljøer. Hvor phishing, malware eller stjålne adgangs-oplysninger ofte kræver interaktion fra brugere, kan en kritisk sårbarhed i nogle tilfælde give direkte adgang til et system. Derfor følger både cyberkriminelle, ransom-waregrupper og andre trusselsaktører nøje med, når nye sårbarheder offentliggøres. Jo større værdi et system har, og jo flere organisationer der anvender det, desto mere attraktiv bliver sårbarheden typisk.

Sårbarheder i VPN-udstyr er derfor særligt interessante, da VPN-løsninger spiller en central rolle i mange organisationers infrastruktur. De bruges til at give medarbejdere, konsulenter og samarbejdspartnere sikker adgang til interne systemer og data. Netop derfor er de også attraktive mål for ondsindede aktører. Hvis en angriber opnår kontrol over VPN-udstyr, kan det i nogle tilfælde give adgang bag netværkets perimeter og dermed omgå en række traditionelle sikkerheds-kontroller. Samtidig er VPN-løsninger ofte forbundet med en høj grad af tillid i organisationen, da de fungerer som en legitim adgangsvej til interne ressourcer.

I nogle miljøer er VPN-udstyr desuden mindre overvåget end eksempelvis servere, arbejdsstationer og endpoints. Det kan gøre det vanskeligere at opdage kompromittering

og give angribere mulighed for at skjule aktivitet over længere tid. I værste fald kan kompromitteret netværksudstyr anvendes til at skjule trafik, ændre logning eller etablere vedvarende adgang til miljøet.

Historisk har ondsindede aktører gentagne gange rettet deres opmærksomhed mod forskellige typer VPN- og fjernadgangsløsninger. Det skyldes blandt andet, at disse teknologier ofte fungerer som en central adgangsvej til organisationers interne systemer og derfor kan give stor værdi for en angriber ved en vellykket kompromittering.

Hvad fortæller scanningerne os?

De observerede scanninger peger på et mønster, der i stigende grad kendetegner det nuværende trusselsbillede. Når der offentliggøres information om en ny sårbarhed, reagerer angribere ofte inden for få timer. Offentligt tilgængelig PoC-kode bliver hurtigt omsat til operationel aktivitet, hvor aktører søger efter eksponerede og sårbare systemer i stor skala. Observationerne indikerer, at både opportunistiske og mere organiserede aktører hurtigt omsætter offentlig tilgængelig viden til konkrete angrebsaktiviteter.

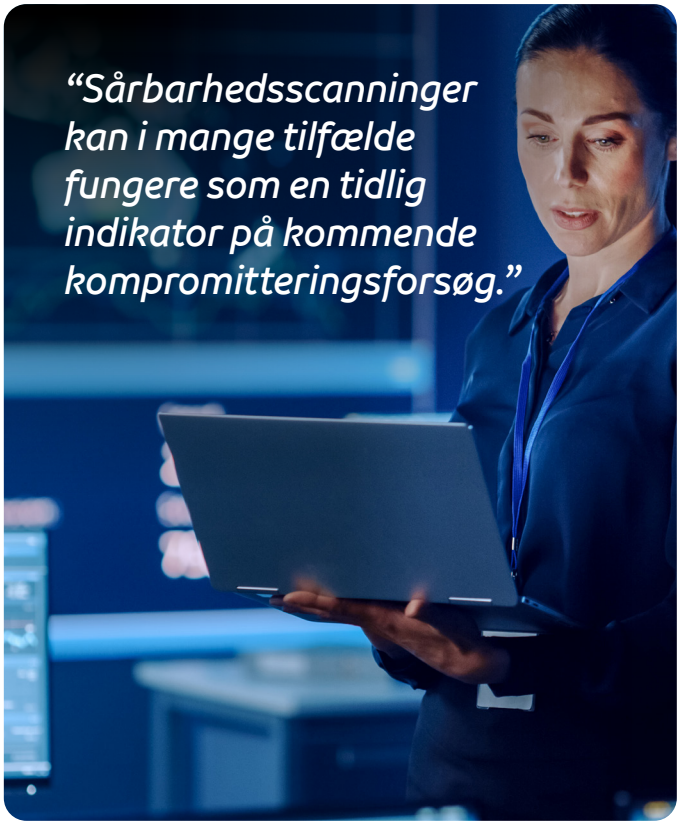
Samtidig viser observationerne, at risikoen ikke nødvendigvis forsvinder, når producenten frigiver en sikkerhedsopdatering. Tværtimod fortsætter både scanninger og aktivitet, som kan indikere forsøg på udnyttelse af sårbarhederne, ofte i uger eller måneder efter offentliggørelsen af patches. Risikoen reduceres derfor ikke umiddelbart, blot fordi en opdatering er blevet gjort tilgængelig.

Årsagen er enkel: Mange organisationer opdaterer ikke deres systemer med det samme. Derfor eksisterer der ofte et betydeligt vindue, hvor sårbarheder fortsat kan udnyttes, selvom en løsning er tilgængelig. Observationerne understreger vigtigheden af, at organisationers patchprocesser tager udgangspunkt i det aktuelle trusselsbillede, så sårbarheder med aktiv scanning og kendt udnyttelse prioriteres højt. Det betyder samtidig, at sårbarhedsscanninger i mange tilfælde kan fungere som en tidlig indikator på kommende kompromitteringsforsøg. Når en bestemt sårbarhed pludselig tiltrækker massiv scanneraktivitet, fortæller det noget om, hvilke systemer og teknologier angriberne aktuelt prioriterer.

Hertil ser vi også, at aktiviteten ikke kun opstod efter offentliggørelsen af PoC-koden. Der blev også registreret scanninger før den offentlige frigivelse, hvilket kan indikere en strategi, hvor aktørerne først identificerer potentielt sårbare systemer og senere vender tilbage for at udnytte dem. Denne tilgang kaldes ofte identify now, exploit later.

AI kan accelerere udviklingen yderligere

Den udvikling bliver endnu mere relevant med fremkomsten af såkaldt Agentic AI, hvor AI-agenter i stigende grad kan planlægge og udføre flere trin i en angrebskæde med begrænset menneskelig involvering. AI kan dermed potentielt automatisere dele af det arbejde, som tidligere



krævede betydelig manuel indsats – eksempelvis at identificere sårbare systemer, undersøge mål og tilpasse angrebsforsøg.

Det betyder ikke nødvendigvis, at AI skal finde nye og ukendte sårbarheder. Tværtimod kan allerede kendte sårbarheder og eksisterende angrebsteknikker sættes sammen og udnyttes systematisk på en skala og med en hastighed, som er vanskelig for mennesker at matche. Det kan samtidig sænke den tekniske barriere for at gennemføre mere målrettede angreb, fordi flere dele af angrebsprocessen kan automatiseres. Det gælder eksempelvis skræddersyet phishing, rekognoscering af potentielle mål og forsøg på at udnytte kendte sårbarheder.

Det gør observationerne fra Q2 relevante også i et fremadrettet perspektiv. Når vi ser trusselsaktører scanne efter kendte sårbarheder på tværs af mere end 1.000 danske organisationer, viser det, hvor mange potentielle mål der kan være interessante, når en sårbarhed bliver aktivt jagtet. I takt med at AI kan automatisere og koordinere flere dele af angrebskæden, kan sådanne eksisterende sårbarheder potentielt udnyttes hurtigere og mere systematisk.

Det kan samtidig ændre økonomien i cyberkriminalitet. Når flere dele af angrebet kan automatiseres, bliver det muligt at forsøge sig mod flere organisationer med mindre manuel indsats. Det kan gøre det attraktivt at angribe virksomheder, som tidligere ville have været mindre interessante, fordi omkostningen ved at gennemføre et angreb var for høj i forhold til den potentielle gevinst. For mindre og mellemstore virksomheder kan det være særligt udfordrende, fordi de ofte har færre ressourcer til at overvåge, opdage og håndtere automatiserede angrebsforsøg.

For virksomheder betyder det, at arbejdet med at identificere og lukke kendte sårbarheder bliver endnu vigtigere. En sårbarhed behøver ikke være ny for at udgøre en alvorlig risiko – den kan være attraktiv, fordi den er kendt, udbredt og kan indgå som et led i en mere automatiseret angrebskæde.

Hvem bliver ramt?

De observerede scanninger var primært rettet mod mellemstore og store organisationer. Hovedparten af aktiviteten ramte virksomheder med mere end 100 ansatte, mens organisationer med over 1.000 medarbejdere var særligt overrepræsenteret. Det hænger sandsynligvis sammen med, at de berørte VPN-teknologier typisk anvendes i større og mere komplekse it-miljøer.

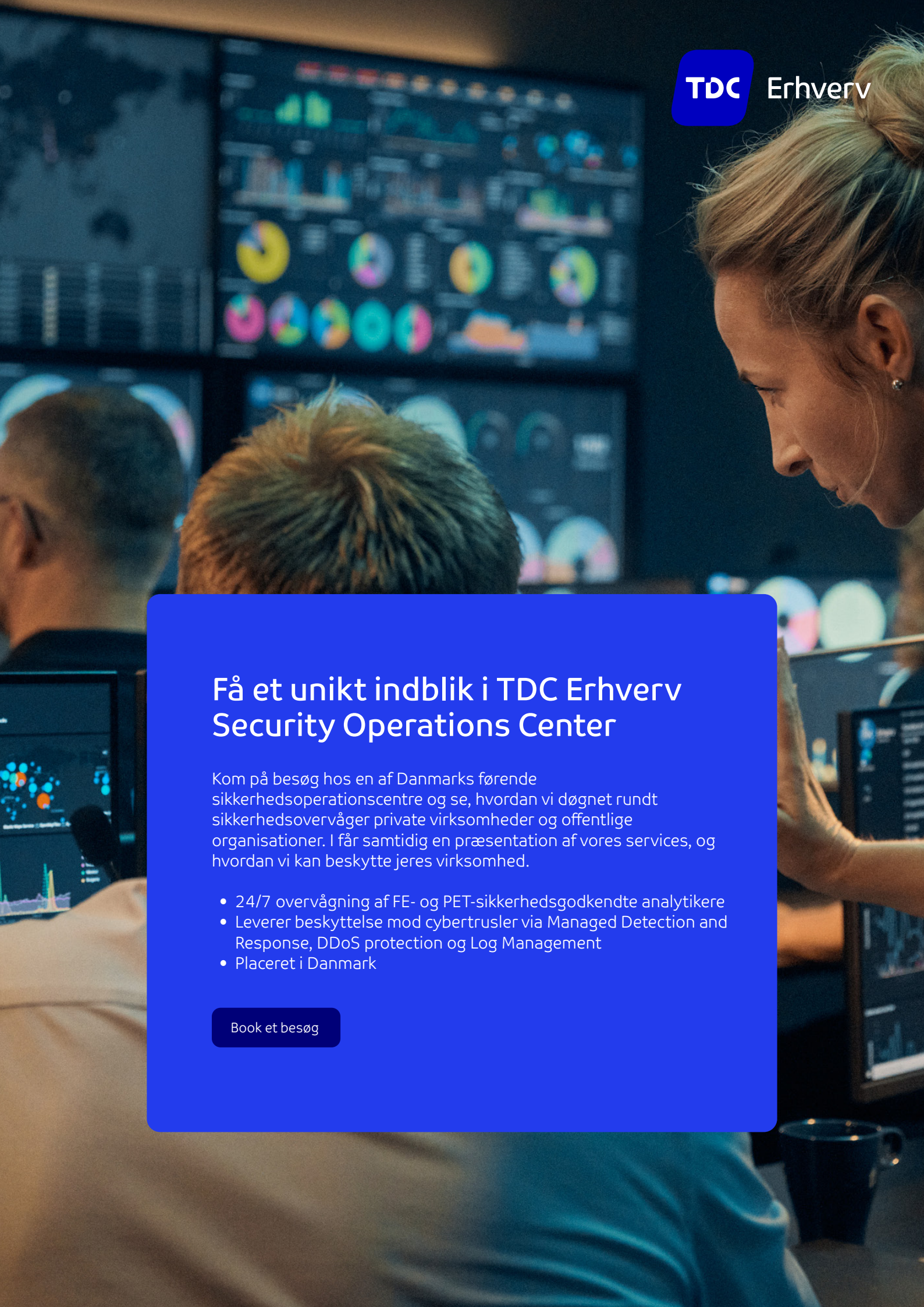
På tværs af de observerede sårbarheder udgjorde virksomheder inden for it-sektoren mellem 18 og 25 % af de scannede organisationer, hvilket gør sektoren til den hyppigst ramte. Samtidig udgjorde organisationer inden for offentlig forvaltning omkring 10 % af de observerede mål. Det understreger, at både private virksomheder og offentlige institutioner fortsat er attraktive mål, når nye sårbarheder opstår i kritisk netværksudstyr.

Fra CVSS-score til trusselsbillede

Traditionelt prioriteres sårbarheder ofte ud fra deres CVSS-score, som angiver den tekniske alvorlighed. Observationerne fra Q2 2026 viser dog, at alvorlighed alene ikke nødvendigvis fortæller hele historien.

Når tusindvis af organisationer bliver scannet for den samme sårbarhed få timer efter offentliggørelsen af et exploit, er det et tydeligt tegn på, at sårbarheden har fanget angribernes interesse. Derfor bør patch management ikke kun tage udgangspunkt i tekniske risikovurderinger, men også i det aktuelle trusselsbillede. Cyber Threat Intelligence-data kan i den sammenhæng fungere som et vigtigt prioriteringsværktøj. Det giver indsigt i, hvilke sårbarheder der aktivt bliver jagtet af angribere netop nu, og kan hjælpe organisationer med at fokusere deres ressourcer der, hvor risikoen er størst.

Kort sagt kan Cyber Threat Intelligence ikke forudsige fremtiden. Men observationerne fra Q2 2026 viser, at data om sårbarhedsscanninger ofte kan give et tidligt billede af, hvilke angreb der potentielt er på vej, og hvilke systemer angriberne har i kikkerten.



TDC Erhverv

Få et unikt indblik i TDC Erhverv Security Operations Center

Kom på besøg hos en af Danmarks førende sikkerhedsoperationscentre og se, hvordan vi døgnet rundt sikkerhedsovervåger private virksomheder og offentlige organisationer. I får samtidig en præsentation af vores services, og hvordan vi kan beskytte jeres virksomhed.

- 24/7 overvågning af FE- og PET-sikkerhedsgodkendte analytikere
- Leverer beskyttelse mod cybertrusler via Managed Detection and Response, DDoS protection og Log Management
- Placeret i Danmark

Book et besøg