TDC Erhverv
Se fremad

TDC Erhverv Sikkerhedsrapporten Q2 2025

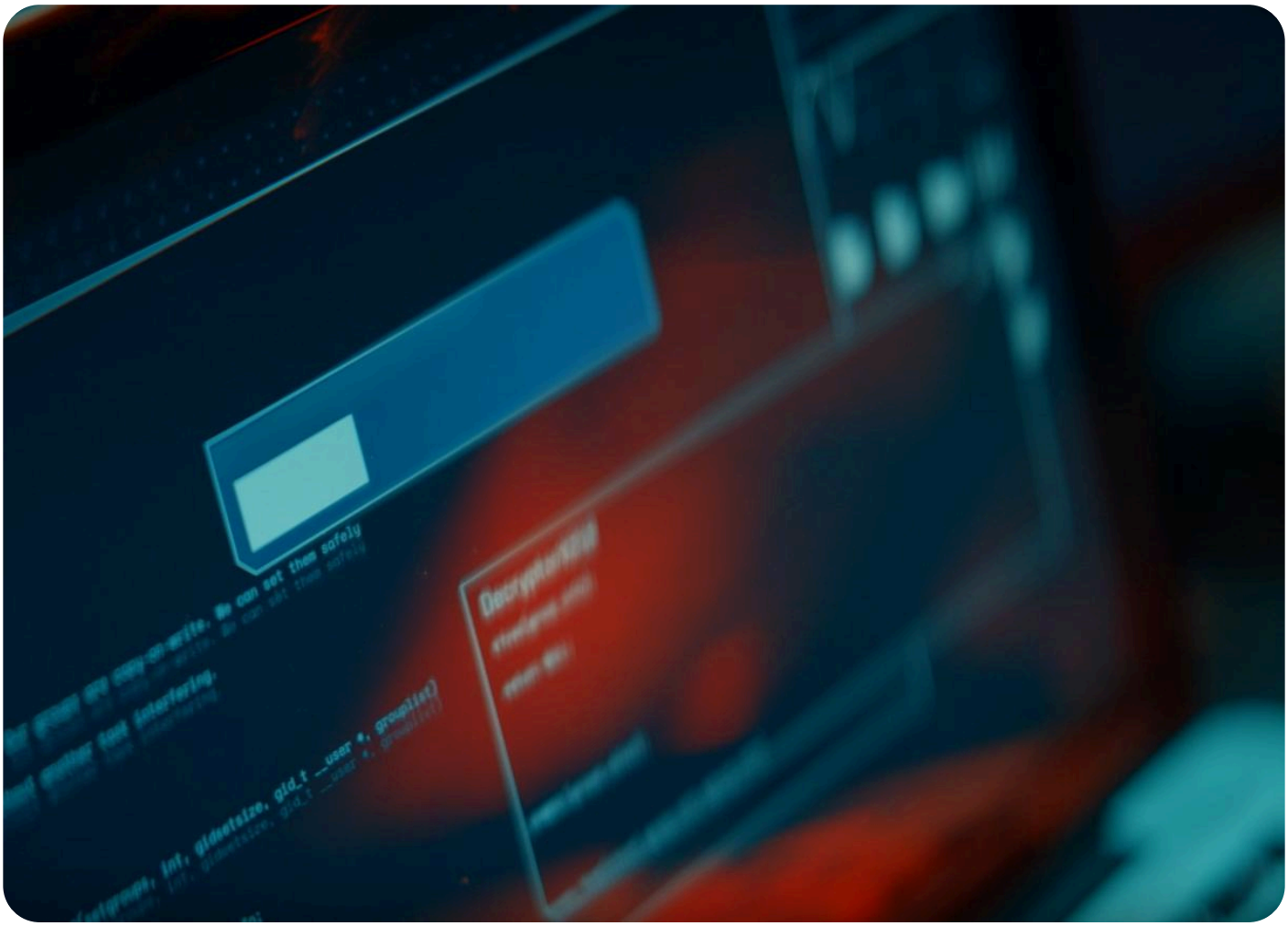
Hvordan håndterede I sikkerheden over sommeren?

Q2 2025 bød på over 5,5 mio. blokerede forsøg på adgang til ondsindede domæner. Over en halv million flere end sidste kvartal og et tydeligt tegn på, at trusselsniveauet ikke sænker sig i takt med at temperaturen stiger. Faktisk tværtimod. Tiden op til sommerferien er typisk højsæson for køb af gode ferietilbud, og her står de cyberkriminelle klar med phishing-angreb skjult bag lokkende tilbud.

Men det er ikke kun volumen, som bør give virksomheder stof til eftertanke. I Q2 så vi en stigning i såkaldte slow-drip-angreb – snigende, lavintensive angreb, der er svære at opdage.

Samtidig trådte NIS2-direktivet i kraft den 1. juli 2025, som hæver barren for, hvad der forventes af virksomheders cybersikkerhed. For dem, der ser længere end minimumskravene, åbner det forretningsmæssige døre: adgang til større og mere sikkerhedsbevidste kunder, mulighed for at byde ind på komplekse udbud og et stærkere brand i en tid, hvor tillid er altafgørende. Med den rette tilgang kan compliance blive en løftestang for både vækst og differentiering.

Læs med, og få indsigt i de trusler og muligheder, der former sikkerhedslandskabet netop nu – og se hvordan I med den rette viden og klare strategiske greb kan styrke jeres position i markedet, selv i en tid med stigende pres og øgede krav.



Q2 2025 i tal

5.518.017

I Q2 2025 registrerede vi over 5 mio. forsøg på at tilgå ondsindede domæner, som blev blokeret af TDC Erhverv Internetfilter. 2.349.314 af blokeringerne skete på kablede forbindelser, mens 3.168.703 skete på mobile forbindelser. Det er en stigning på over en halv million siden sidste kvartal.

Forsøgene er altså mange og fortsat stigende. Virksomheder bør derfor være særligt opmærksomme – også i sommerferieperioderne. Læs videre i rapporten og se, hvordan sommer, sol og sikkerhed kan gå hånd i hånd.

Top 3 trusler i Q2 2025

66,3 % Malware

Malware var igen i Q2 den type trussel, vi oftest blokerede med TDC Erhverv Internetfilter. Vi observerede bl.a. forsøg på angreb med GootLoader – en listig form for malware, der ofte kan infiltrere systemer uden at vække mistanke.

24,55 % Phishing

Phishing kom for første gang i top 3 i Q3 2024 og har siden været en fast genganger. I Q2, hvor sommerferien stod for døren, steg andelen markant til 24,55 %, mod 13,4 % i Q1.

5,95 % C&C (command and control)

C&C har også holdt fast i sin plads i top 3 siden sidste kvartal, og bruges typisk af cyberkriminelle som værktøj til at styre og kontrollere de enheder, de har inficeret med malware eller ondsindet software.

TDC Erhverv Internetfilter: Mere digital tryghed i jeres arbejde – også på farten

Med TDC Erhverv Internetfilter kan medarbejdere arbejde trygt på internettet, uanset hvor de befinder sig. Internetfilter analyserer browsertrafikken og blokerer automatisk besøg på skadelige sider, der kan stjæle data, installere malware eller på anden måde inficere mobiler, computere og tablets.

Læs mere om TDC Erhverv Internetfilter

GootLoader – malwaren der udnytter vores tillid til systemet

GootLoader er en form for malware, vi har observeret flere gange i Q2. Det særlige ved denne type er, at den henter skadeligt software ned til det inficerede system ofte helt uden at blive opdaget, før det er for sent.

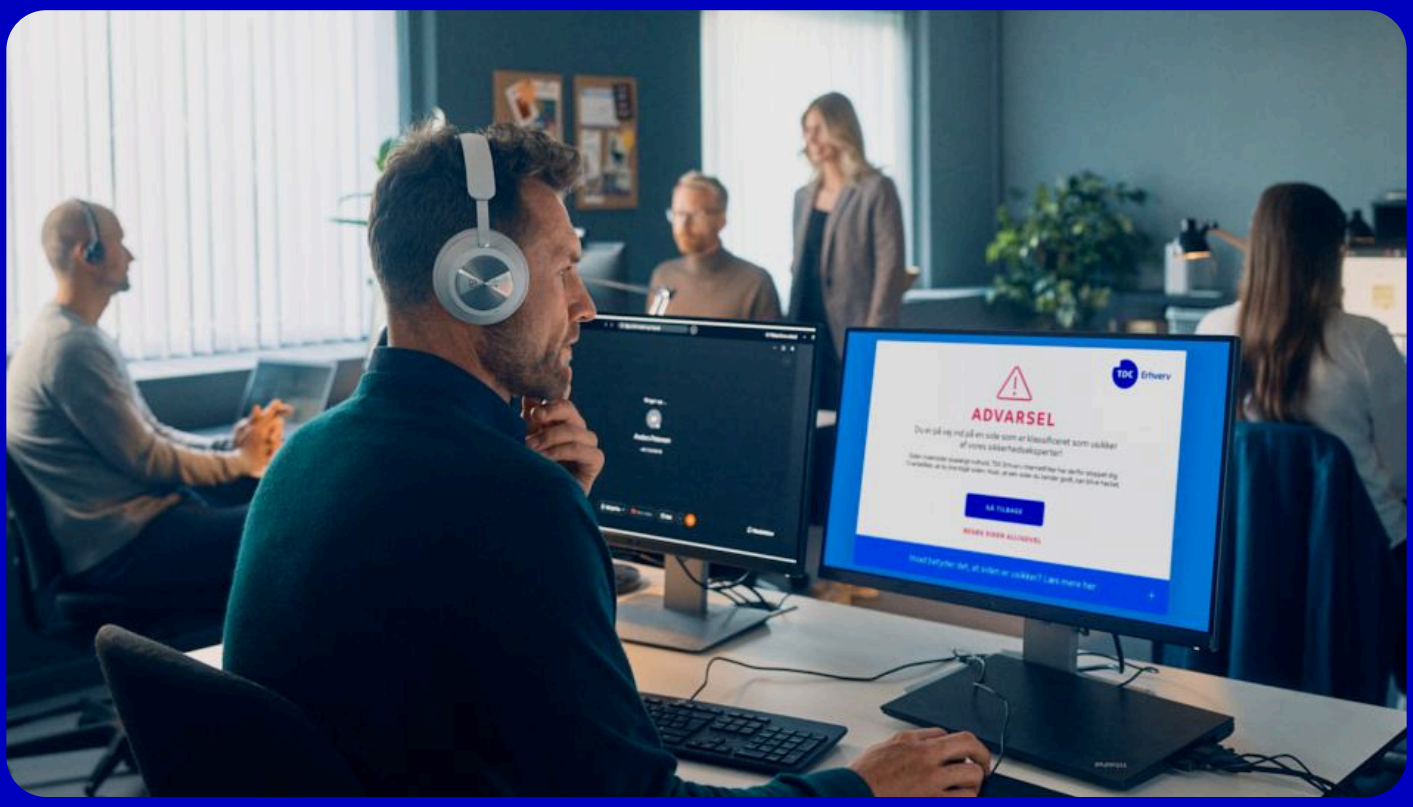
Hvad er en loader?

En loader er et værktøj i malware-økosystemet, der har til formål at hente og starte anden skadelig software på et kompromitteret system, uden at brugeren opdager det. Når først værktøjet har etableret adgang, kontakter det den cyberkriminelles server og henter eksempelvis ransomware, spyware, fjernadgangstrojanere (RATs) eller værktøjer som Cobalt Strike. Sidstnævnte bruges typisk af organiserede cyberkriminelle grupper til at infiltrere organisationer med henblik på at stjæle information eller gøre politisk og økonomisk skade.

Så snedig og sejlivet kan en loader være

GootLoader er et af de mere avancerede eksempler på denne type malware. Ved hjælp af social engineering og SEO-manipulation påvirker den søgeresultaterne for de ramte brugere, så kompromitterede hjemmesider placeres højt i eksempelvis Google-søgninger, når de leder efter juridiske dokumenter, dokumentskabeloner eller lignende. Denne metode kaldes SEO poisoning. Når brugeren klikker på linket og downloader det tilsyneladende legitime materiale, ofte et ZIP-arkiv med en JavaScript-fil, aktiveres loaderen, som henter og kører ondsindet kode i baggrunden.

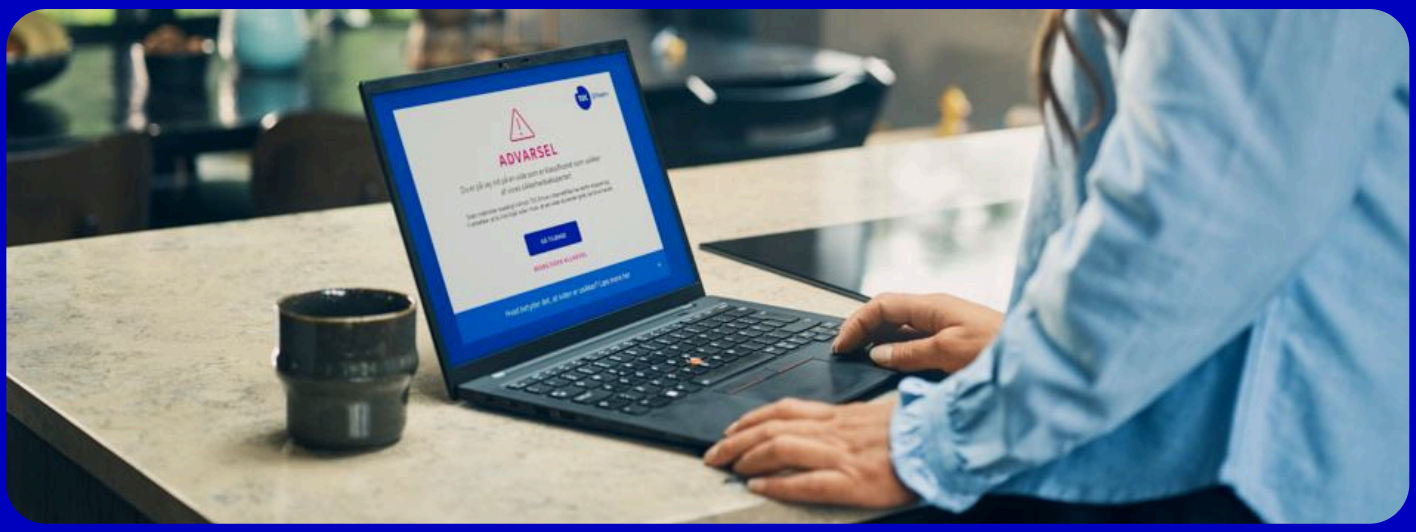
Alt dette sker gennem en kombination af metoder, der er nøje designet til at undgå opdagelse. GootLoader anvender blandt andet scriptbaserede teknikker til at levere malware. Scripts er ofte tilladt og anvendes bredt i virksomheder til automatisering og administration, hvilket gør dem mindre mistænkelige i første omgang. Samtidig udnytter GootLoader eksisterende, godkendte processer i operativsystemet, for eksempel Windows-processer som explorer.exe eller svchost.exe, til at afvikle koden. Den måde, koden leveres, aktiveres og afvikles på, gør det nemmere for den at undgå mistanke hos mange traditionelle sikkerhedsløsninger.



Ekstra foranstaltninger som obfuskering, hvor koden bevidst gøres kompleks og uigennemskuelig, og kommunikation via krypteret netværkstrafik, hvor indholdet ikke umiddelbart kan læses eller blokeres, gør det særligt vanskeligt at analysere og identificere koden som skadelig. Loaderen udgør derfor en væsentlig risiko, da den er svær at opdage og stoppe, når først den er aktiveret.

Hos TDC Erhverv har vi allerede blokeret 15.076 besøg på hjemmesider associeret med denne type malwarekampagne og beskyttet over 1.000 kunder på tværs af brancher mod sådanne angreb. Det understreger, hvordan moderne cybertrusler i dag ikke kun handler om teknisk snilde, men også om evnen til at udnytte menneskelige svagheder og tillid. Når social engineering kombineres med avanceret loader-arkitektur, bliver det lettere for de cyberkriminelle at opnå dyb og ubemærket adgang til netværk og potentielt forretningskritiske data.

Derfor er det afgørende, at virksomheder arbejder proaktivt med sikkerhedsoplysning, adgangskontrol og avanceret detektion for at mindske risikoen. At forstå, hvordan en loader fungerer, er et vigtigt skridt mod at styrke modstandskraften og stå stærkere over for angreb, der hele tiden udvikler sig og tilpasser sig nye forsvarsmekanismer.



Slow-drip: Ikke alle angreb er hurtige og overvældende – men de skal stadig tages alvorligt

Mens traditionelle, store DDoS-angreb ofte fylder i medierne, vinder de mere stille og vedholdende low-and-slow-angreb frem, som er langt sværere at opdage.

I sidste udgivelse af TDC Erhverv Sikkerhedsrapporten dykkede vi ned i DDoS-angreb –en voksende trussel mod både private virksomheder, offentlig infrastruktur og samfundskritiske tjenester. DDoS, eller Distributed Denial of Service, er en form for cyberangreb, hvor aktøren typisk overbelaster en hjemmeside eller netværkstjeneste med en massiv mængde trafik, for at få systemet til at gå ned eller blive utilgængeligt for de legitime brugere, der forsøger at tilgå det.

Sådanne angreb er normalt kendetegnet ved at være hurtige og kraftige for at overvælde systemet. Men her i Q2 har både vi og vores partner Whalebone en europæisk cybersikkerhedsspecialist med fokus på DNS-beskyttelse - observeret en anden form for DDoS-angreb, der adskiller sig markant fra den klassiske metode: slow-drip.

Subtile angreb med mærkbare effekter

Slow-drip-metoden sender kun en lav mængde trafik, men over en længere periode og med præcis timing, for gradvist at udmatte serverressourcer (fx forbindelser, hukommelse eller processorkraft). Selvom angrebene ikke forårsager komplet nedlukning af services, kan de med tiden påvirke virksomheder og offentlige tjenesters drift og systemer.

For virksomheder og offentlige tjenester, der er afhængige af at være gnidningsfrie og altid tilgængelige, er det derfor mindst lige så vigtigt at være forberedt på disse subtile angreb som på de store trafikbølger.

Svær at spotte med traditionelle sikkerhedsmetoder

Den lille mængde data, som slow-drip-metoden anvender, imiterer normal trafik fra 'langsomme' brugere eller ustabile forbindelser. Da mange overvågningsværktøjer primært fokuserer på trafikmængder, kan angrebet let overses.

Metoden kræver heller ikke store botnets og er derfor attraktiv for mindre ressourcestærke angribere, hacktivister og cyberkriminelle grupper. Det gør den nemt udbredt og kan bruges flittigt til at ramme virksomheder og offentlige tjenester.

Det understreger behovet for en flerlaget tilgang til DDoS-beskyttelse, hvor cloudbaserede løsninger kombineres med dedikerede on-premise-systemer for effektivt at imødegå avancerede angrebsteknikker som low and slow.

> Hos TDC Erhverv rådgiver vi om den optimale sammensætning af løsninger og arbejder tæt sammen med vores kunder for at styrke hele deres sikkerhedsarkitektur – både lokalt og i skyen.

Går jeres it-afdeling på ferie? Det gør de cyberkriminelle ikke

Af Lars Højberg
Chef for Security Operations Center i TDC Erhverv

Det danske samfund er et af de mest digitaliserede i vor tid, og med det følger en høj cybertrussel, som gør danske virksomheder sårbare. Det kræver særlig bevågenhed og parathed at modstå de uundgåelige cyberangreb – især op til ferieperioder, hvor paraderne ofte sænkes.

Historisk set har vi i TDC Erhverv observeret nogle tydelige tendenser hen over foråret. I Q2 2025 registrerede vi for eksempel 5,5 mio. blokeringer med TDC Erhverv Internetfilter sammenlignet med blot 3 mio. i Q3 2024.

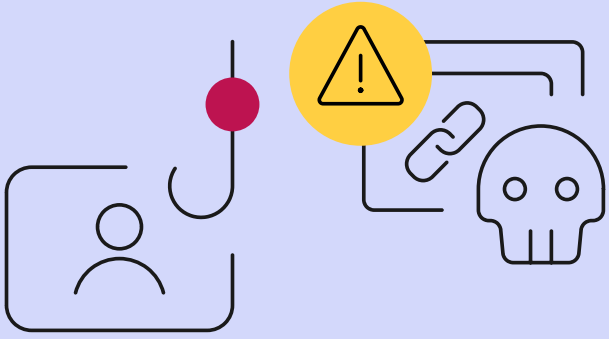
Det kan blandt andet skyldes, at mange i Danmark i denne periode er på udkig efter gode tilbud på flybilletter, hoteller og oplevelser til sommeren. Det fører til flere klik og køb både fra arbejdscomputere og -telefoner og fra private enheder. Her ser vi, at når fokus er på ferie og ikke på sikkerhed, bliver det nemmere for cyberkriminelle at lokke brugere i fælden med falske mails og tilbud, der fremstår troværdige.

I Q2 i år var antallet af phishing-angreb markant stigende, drevet af de mange muligheder for at lokke feriespændte købere i fælden. Det er en trussel, der i værste fald kan give cyberkriminelle adgang til at implementere ransomware og udnytte virksomheden økonomisk.

Med de historiske tendenser for øje er det derfor særligt vigtigt at være beredt i tiden op til de store ferieperioder.

Her kan viden og sund adfærd være jeres vigtigste værn, for eksempel gennem træning af medarbejdere i at spotte falske tilbud og hjemmesider. Det kræver dog både tid og dyrebare ressourcer, typisk i form af kurser, tests og løbende påmindelser, og selv da er det ikke et skudsikkert værn. Med stadig mere avancerede metoder kan cyberkriminelle udforme mails og hjemmesider, der er næsten umulige at skelne fra de ægte. Der skal kun få uopmærksomme klik til fra en ellers veltrænet medarbejder, før et sikkerhedsbrud kan opstå.

Kigger vi alene på antallet af blokeringer med TDC Erhverv Internetfilter over tid, er det tydeligt, at der er en stigende tendens til, at brugere landet over ryger i fælden. Hver blokering er en potentiel redning fra et sikkerhedsbrud hos vores kunder og understreger behovet for et ekstra lag af beskyttelse, som træder til, når brugeradfærden svigter.



Hvad havde I gjort i juli, hvis uheldet var ude?

Når sommerferien endelig er over os, og medarbejderne tager velfortjent fri, gælder det som regel også it-afdelingen. Men mens it-sikkerheden måske kører på lavt blus, er truslen alt andet end på ferie.

Sammenlignet med Q1 & Q2 (2024) så vi i Q3 2024 et fald i blokeringer med TDC Erhverv Internetfilter, hvilket fulgte det typiske fald i aktivitet på arbejdscomputere og -telefoner. Vi så til gengæld en stigning i andelen af både malware- og phishingforsøg. Man er altså ikke fredet over sommeren. Virksomheder skal være på vagt og klar til at reagere hurtigt.

Men det kan være svært, når it-afdelingen er på ferie og potentielt i flere uger. Virksomheder med kun én eller få specialister må ofte sende dem afsted og håbe, at intet sker – med deres private telefonnumre skrevet ned, bare for en sikkerheds skyld. Virksomheder med flere ressourcer i it-afdelingen har mulighed for at forskyde ferieperioderne for nøglemedarbejdere, men selv da kan kombinationen af ferie, sygdom og uforudsete hændelser betyde, at virksomhedens sikkerhed i perioder står uden sine vogtere.

I disse perioder kan en ekstern it-sikkerhedspartner være forskellen på en fredelig sommer og begyndelsen på en svær kamp. Det frigiver også interne it-ressourcer, som i stedet kan bruges på kernopgaver som udvikling og skalering. Og vigtigst af alt giver det ro til at sende it-afdelingen på ferie med visheden om, at sikkerheden aldrig holder fri.

Er I godt rustet til at modstå truslerne?

Svar på 14 spørgsmål fordelt på 6 temaer inden for it-sikkerhed, og få kortlagt jeres virksomheds it-sikkerhedsprofil. Så kan I se, om I er rustet til at modstå truslerne – og håndtere situationen, hvis uheldet er ude. Testen er uforpligtende, og I får resultatet med det samme.

Tag testen

Fra compliance til konkurrencefordel: Sådan kan NIS2 løfte forretningen

Claus Westergaard Kraft
Direktør for Cybersikkerhed & Cloud i TDC Erhverv

Sikkerhed er ikke kun et krav og en nødvendig udgift. Det er et løfte til jeres kunder og til samfundet – og et strategisk springbræt til øget resiliens og differentiering.

For mange virksomheder betragtes cybersikkerhed blot som en omkostning, en nødvendig forsikring mod bøder og nedetid, og endnu et punkt på direktionens lange liste over prioriteringer.

I en digital verden, hvor tillid og fleksibilitet er afgørende konkurrenceparametre, er cybersikkerhed ikke bare en forudsætning – det er et vækstpotentiale.

Med det nye NIS2-direktiv, som trådte i kraft den 1. juli 2025, bør de skærpede krav til cybersikkerhed ikke blot ses som endnu en compliance-øvelse og regulatorisk forpligtelse, men som en kærkommen invitation til at løfte cybersikkerheden, og derigennem virksomheden, til et nyt niveau.

Fra taktiske tiltag til forretningsdrevne investeringer

Når I som virksomhed vælger at gå længere end minimumskravene, viser I handlekraft og modenhed til at navigere sikkert, også når trusselsbilledet ændrer sig. I fremstår som en sikker og kompetent partner og en stærk spiller over for kunder, partnere, myndigheder og samfundet. Det åbner for nye forretningsmuligheder, herunder adgang til større og mere sikkerhedsbevidste kunder, deltagelse i komplekse forsyningskæder og et styrket brand.

- **Styrk jeres governance og ledelsesforankring**
  Ved at etablere et dedikeret cybersikkerhedsudvalg i bestyrelsen sender I et klart signal til kunder og samarbejdspartnere om, at I tager sikkerhed alvorligt helt op på topledelsesniveau. Det skaber tillid og demonstrerer modenhed, hvilket kan være afgørende, når I deltager i udbud og indgår nye partnerskaber.
- **Invester i moderne teknologier og arkitektur**
  Med en stærk teknisk sikkerhedsgrundstruktur reducerer I risikoen for driftsstop og datatab. Det betyder færre afbrydelser og en mere stabil serviceoplevelse. Start med at få mest muligt ud af de løsninger, I allerede har – mange udnytter fx ikke de sikkerhedsfunktioner, der følger med deres Microsoft-licens. Supplér derefter med tiltag som Zero Trust og netværkssegmentering, der effektivt kan begrænse et angreb. Det gør jer mere attraktive for kunder, der forventer høj tilgængelighed og forudsigelighed.
- **Skab en stærk sikkerhedskultur, der gennemsyrer hele organisationen**
  Med en security-first-tankegang, hvor alle i virksomheden forstår deres rolle i at beskytte virksomheden, bliver sikkerhedsprocedurer en naturlig del af hverdagen og ikke blot en compliance-øvelse. Det minimerer menneskelige fejl og signalerer ansvarlighed over for både kunder og partnere.
- **Gå det ekstra skridt og vær gennemsigtige omkring det**
  Ved at gå ud over NIS2-direktivets krav og følge internationale standarder som for eksempel ISO 27001 – og lade jer certificere, hvor det er muligt, står I ikke blot stærkere på cybersikkerheden, men differentierer jer også fra konkurrenterne og bliver førstevalget for kunder, der prioriterer sikkerhed højt. Det åbner samtidig døren til nye markeder og giver adgang til offentlige og internationale udbud, hvor kravene til sikkerhed og dokumentation er skærpede.

Det sætter krav til hele ledelsen – ikke kun it-chefen

For at realisere potentialet i NIS2 kræver det, at cybersikkerhed løftes fra it-afdelingen og ind i hjertet af forretningen. Sikkerhed bør ikke ses som et isoleret teknisk ansvar, men som en integreret del af forretningsstrategien. Når topledelsen tager aktivt ejerskab, kan cybersikkerhed blive en del af de centrale strategiske beslutningsprocesser og udvikle sig fra et nødvendigt værn til en drivkraft for langsigtet vækst.

Med NIS2 står erhvervslivet over for et valg: Skal cybersikkerhed ses som en byrde, eller som en platform for en fremtidssikret og konkurrencedygtig forretning?

Zero Trust – hvor intet overlades til tilfældelighederne

Traditionelt har mange virksomheder arbejdet ud fra idéen om en sikker perimeter, hvor alt og alle inden for virksomhedens netværk automatisk anses som troværdige. Men med øget fjernarbejde, cloud-løsninger og mere avancerede trusler er denne tilgang ikke længere tilstrækkelig.

Zero Trust er en moderne sikkerhedsstrategi, der blandt andet bygger på kontinuerlig verifikation af både interne og eksterne brugere ved adgang til systemer samt segmentering af netværket. Det reducerer risikoen for angreb udefra og begrænser skaderne, hvis cyberkriminelle alligevel får adgang.

Læs mere om Zero Trust og andre moderne tilgange til datasikkerhed i vores whitepaper:
Morgendagens data-sikkerhed skabes i dag.

Download whitepaper

TDC Erhverv
Se fremad

Skal et af Danmarks førende sikkerhedsoperationscentre have jeres ryg næste sommer?

TDC Erhverv Security Operations Center overvåger netværk for både private og offentlige kunder. Se, hvordan vi også kan beskytte jeres virksomhed.

- 24/7 overvågning udført af FE- og PET-sikkerhedsgodkendte analytikere
- Leverer beskyttelse mod cybertrusler via stærk Managed Detection Reponse, DDoS protection og Log Management
- Placeret i Danmark, så jeres data forbliver på dansk jord

Læs mere om TDC Erhverv SOC