

GUIDE

Byg din digitale **modstandskraft**

Din guide til en sikrere og mere modstandsdygtig virksomhed.

advania

The tech company
with people at heart

Hvordan ville jeres organisation klare sig, hvis IT-systemerne var nede i 48 timer?

For mange ville konsekvenserne være omfattende. Leverancer kunne gå i stå, kunder blive påvirket, og vigtige beslutninger forsinkes.

I takt med at næsten alt i vores samfund og vores virksomheder bliver digitalt, øges også antallet af angrebspunkter, som gør os sårbare over for trusler. Digital modstandskraft handler om evnen til at modstå, reagere på og hurtigt komme sig efter det uventede.

Det er ikke kun et spørgsmål om teknologi, men også om mennesker, processer og lederskab – alt sammen faktorer, der tilsammen styrker beskyttelsen mod cybertrusler og driftsforstyrrelser.

I denne guide har vi samlet **fem grundlæggende områder**, der kan hjælpe dig og dine medarbejdere med at styrke jeres digitale modstandskraft.

Se helheden: **mere end bare en teknikløsning**

Gennemgå, hvordan I arbejder inden for følgende områder:

- **Teknologi og infrastruktur:** Er systemerne opdaterede og beskyttede?
- **Organisation og lederskab:** Findes der tydelige roller og ansvarsområder?
- **Mennesker og adfærd:** Har medarbejderne den rette viden?
- **Processer og procedurer:** Ved I, hvem der gør hvad ved et indbrud?
- **Leverandørkæder og partnerskaber:** Hvor sikre er jeres samarbejder?

Afhængigt af hvilket område der skal gennemlyses, kan jeres virksomhed få hjælp gennem:

- Rådgivning og strategi, f.eks. risikoanalyser, styringsmodeller og udvikling af politikker.
- Ledelsesforankring, f.eks. uddannelse af ledergrupper om ansvar og risikoejerskab.
- Helhedsforvaltning, f.eks. et sikkerhedsoperationscenter (SOC), der overvåger og håndterer hændelser i realtid.
- Certificeringsstøtte – hjælp til at opfylde nye regler og standarder (fx NIS2, CRA, ISO 27001).



Træn sikre **adfærdsmønstre**

Størstedelen af alle databrud starter med en menneskelig fejl. Det kan handle om, at man fra begyndelsen har valgt et svagt kodeord, eller at man har klikket på et forkert link eller foretaget en uovervejet filhentning. De fleste af os har nok både privat og på arbejdet modtaget e-mails, der allerede ved første øjekast virkede mistænkelige. Ofte reagerer vi på et mærkeligt sprog, stavefejl eller en afsenderadresse, der ikke ser ægte ud. Men med hjælp fra AI er disse phishing-mails blevet stadig mere avancerede, hvilket gør det svært for mange at skelne mellem ufarlige og farlige e-mails. Ved at træne medarbejderne til at agere sikkert i hverdagen opbygger du en stærk sikkerhedskultur, der holder – også når hverdagen bliver travl og presset.

I kan for eksempel træne på:

- Simulerede phishingøvelser for at øve realistiske situationer.
- Tilpassede uddannelsesprogrammer, der tager udgangspunkt i brugerens risikoadfærd.
- Gamification og positiv feedback, hvor sikkerhed bliver en naturlig del af hverdagen og ikke kun en kontrolfunktion.



Brug AI for at **styrke dit forsvar**

I dag udvikler cybertruslerne sig hurtigt, og angribere bruger ofte AI til at finde nye veje ind. Men den samme teknologi kan bruges til at beskytte din virksomhed.
Den nye generation af AI-systemer anvender kunstig intelligens og maskinlæring til hurtigere at identificere afvigelser i store datamængder. Den kan også registrere mønstre, der ligner dem fra tidligere angreb.
Ved at bruge AI-drevne sikkerhedsløsninger kan du opdage trusler hurtigere, reducere antallet af falske alarmer og reagere i tide.

Kort sagt kan AI bruges til at styrke dit cyberforsvar – især mod angribere, der selv bruger AI.

Nogle eksempler på løsninger er:

- XDR-systemer (Extended Detection & Response), som er integrerede sikkerhedssystemer, der sammenkobler forskellige typer sensorer og datastrømme og analyserer afvigelser i realtid.
- Security Copilot-løsninger, som er AI-assistenter, der understøtter og styrker sikkerhedsteamenes daglige arbejde.
- SOC-as-a-Service, som er et alternativ, hvor man ikke anvender virksomhedens egne IT-ressourcer, men outsourcer døgnbemandet overvågning og hændelseshåndtering til en tredjepart.

Beskyt din virksomhed gennem **sikre partnerskaber**

At bruge leverandører og partnere er en selvfølge i mange virksomheder. Men man bør også tage højde for, at det kan medføre risici. Derfor er det vigtigt at arbejde struktureret med at kortlægge, hvilke potentielle sikkerhedsrisici hver leverandør kan medføre.

Start med at:

- Kortlægge og kvalificere alle leverandører ud fra deres risikoniveau.
- Stille tydelige sikkerhedskrav og løbende følge op på, at de efterleves.
- Formulere og dokumentere sikkerhedsprocedurer i aftaler, så roller, ansvar og tiltag er klart defineret i tilfælde af hændelser.

Har jeres virksomhed brug for hjælp til dette, kan man for eksempel gøre brug af:

- TPRM (Third Party Risk Management-programmer), som er et systematisk rammeværk til at vurdere og gennemgå leverandører.
- Sikker integration af cloudtjenester, som understøtter jer i beslutninger, konfigurationer og selve driften af jeres cloudløsninger.



Gør regelefterlevelse til en **naturlig del af hverdagen**

Teknologi og datahåndtering udvikler sig i et hæsblæsende tempo. Derfor er det måske ikke så mærkeligt, at også regelværk og compliance-krav ændrer sig med jævne mellemrum. Men reglerne kan blive stadig mere komplekse at både fortolke og implementere. For at lykkes er det nødvendigt, at compliance bliver en naturlig del af det løbende sikkerhedsarbejde — og ikke blot et isoleret, midlertidigt projekt.

Sådan kan du komme i gang:

- Compliance-as-a-Service, det vil sige, færdige pakker, der hjælper dig med at leve op til regelværk som fx NIS2, ISO, DORA m.fl.
- Modenhedsanalyser, der giver en vurdering af din virksomheds nuværende sikkerhedsniveau og identificerer de rigtige prioriteringer.
- Dokumentation og rapportering, som skaber grundlag for eventuelle opfølgninger fra myndigheder.



Sammanfatning:
Sådan bygger I digital modstandskraft

Start med at:

- Identificere jeres mest kritiske aktiver.
- Uddanne medarbejderne i sikker adfærd.
- Etablere procedurer for håndtering af sikkerhedshændelser.
- Sikre jeres økosystem af partnere og leverandører.
- Gennemgå jeres arbejde med efterlevelse af regler og standarder.

Vil du vide, hvor din virksomhed står i dag?

Kontakt Advania for en første modenhedsanalyse eller rådgivning inden for digital robusthed.

Kontaktoplysninger

Web: advania.dk

E-mail: info@advania.dk

Telefon: +45 39 48 48 00

advania

The tech company
with people at heart