En guide til IT-sikkerhed, som alle kan forstå

Medarbejdernes rolle - Fra det svageste led til det stærkeste.

USER IT

Mange virksomheder er i dag blevet bedre til at håndtere IT-sikkerhed. De fleste har styr på de tekniske grundelementer: firewalls er installeret, antivirusprogrammer er opdaterede, og der tages regelmæssig backup af virksomhedens dokumenter.

Men giver det overhovedet mening at investere i disse tekniske løsninger, hvis vi overser den største risikofaktor?

Faktum er, at **omkring 95 % af IT-sikkerhedsbrud skyldes menneskelige fejl** – ikke tekniske svagheder. Det understreger behovet for en stærk sikkerhedskultur, hvor medarbejderne er bevidste om deres rolle i at beskytte virksomhedens data.

Når man taler om IT-sikkerhed, kan det for mange virke abstrakt.
Hvad indebærer det egentlig? Hvilke konsekvenser kan det få, hvis man ikke tager det alvorligt?

Ét er sikkert: En stærk sikkerhedskultur reducerer risikoen for brud markant, fordi medarbejderne får bedre vaner og større bevidsthed.

Hvad er kultur?

På en arbejdsplads udvikler der sig over tid en særlig måde at gøre tingene på – en slags fælles forståelse eller praksis, som ofte bliver en naturlig del af hverdagen. Denne arbejdspladskultur kan afspejle sig i alt fra små vaner, som hvornår medarbejderne typisk møder ind, til større spørgsmål som graden af fleksibilitet i forhold til hjemmearbejde.
Når en mindre gruppe kolleger begynder at handle på en bestemt måde, er det meget sandsynligt, at resten af organisationen gradvist vil følge trop.

Kulturen former sig i praksis – ikke gennem regler, men gennem adfærd.

På samme måde bør IT-sikkerhed ikke blot være en teknisk foranstaltning, men en integreret del af virksomhedens kultur.

Hvad er en sund IT-sikkerhedskultur?

En virksomheds sikkerhedskultur handler om, hvorvidt sikkerhed er noget, man taler om, prioriterer og tager ansvar for i dagligdagen. Det er ikke kun noget, der står i en politik i intranettet, men noget der kan mærkes i de handlinger, beslutninger og vaner, medarbejderne har i deres digitale arbejdsliv.

Sikkerhedskultur bliver formet over tid – gennem ledelsens signaler, de samtaler vi har med hinanden, og de erfaringer vi gør os. Det kræver løbende opmærksomhed at udvikle og vedligeholde en kultur, hvor sikkerhed ikke er noget, man først tænker over efter et problem opstår.

Hvordan ser en stærk sikkerhedskultur ud?
I en virksomhed med en stærk sikkerhedskultur vil medarbejderne ofte:

- Tage ansvar for at beskytte data og systemer i deres daglige arbejde.
- Være opmærksomme på mistænkelig aktivitet – og melde det videre.
- Hjælpe hinanden med at undgå IT-trusler, f.eks. ved at dele viden om phishing.
- Føre åbne samtaler om sikkerhed – uden frygt for at stille "dumme" spørgsmål.
- Følge virksomhedens sikkerhedspolitikker, fordi de forstår *hvorfor* de findes.

Hvordan ser en svag sikkerhedskultur ud?
I modsætning hertil vil man i virksomheder med en svag sikkerhedskultur ofte opleve, at:

- Sikkerhed bliver opfattet som noget, kun IT-afdelingen tager sig af.
- Der sjældent tales om IT-sikkerhed, medmindre noget går galt.
- Adgangskoder deles eller genbruges.
- Mistænkelige e-mails ignoreres – eller endda klikkes på uden omtanke.
- Medarbejdere tager risici, f.eks. ved at bruge offentlige Wi-Fi-netværk med arbejdsenheder.

Hvorfor en stærk sikkerhedskultur gør en forskel

Mange tror, at IT-sikkerhed handler om teknik, men det starter med mennesker.

Når nu de fleste databrud skyldes menneskelige fejl, er det afgørende at fokusere på medarbejdernes adfærd og vaner. En stærk sikkerhedskultur gør det lettere at tage ansvar, stille spørgsmål og reagere på det, der virker forkert.

Det handler ikke om at være ekspert, men om at være opmærksom og tryg ved at sige noget højt – også når man er i tvivl.

IT-afdelingen har et ansvar, men det fritager ikke os andre.

Vi skal kunne genkende faresignaler og vide, hvornår vi skal reagere – ligesom vi kontakter en læge, når kroppen føles forkert.
Når alle har lidt viden og tør sige noget, opdager vi problemer i tide – *og det kan gøre en stor forskel.*

Hvad svækker en sund sikkerhedskultur?

Selv den bedste intention om at skabe en stærk sikkerhedskultur kan blive udfordret af hverdagen. Der er nemlig flere faktorer, som stille og roligt kan underminere det fælles fokus på IT-sikkerhed – ofte uden man opdager det med det samme.

Her er nogle eksempler på situationer, der kan spænde ben for kulturen:

Forvirrende regler og teknisk sprog

Hvis IT-politikkerne er fyldt med lange afsnit, forkortelser og tekniske krav, som ikke bliver forklaret, vil mange stå af. Jo mere komplekst det føles, jo større er risikoen for, at reglerne bliver ignoreret i en travl hverdag.

Når hurtighed vinder over sikkerhed

En kultur, hvor det vigtigste er at blive hurtigt færdig, kan føre til, at man "bare lige" klikker på et link i en mail uden at tænke sig om. Når tempo og produktivitet vægtes højere end forsigtighed, ryger sikkerheden nemt i baggrunden.

Sikkerhed er usynligt i ledelsen

Hvis man aldrig hører ledelsen nævne IT-sikkerhed, og der sjældent bliver sat tid eller budget af til det, er det svært at forvente, at medarbejderne tager det seriøst. Kulturen bliver præget oppefra – og hvis der ikke signaleres, at sikkerhed er vigtigt, smitter det hurtigt af.

Konstant udskiftning i medarbejdergruppen

Virksomheder med høj udskiftning eller mange vikarer oplever ofte, at det er svært at forankre en kultur. Nye medarbejdere skal oplæres, og de når sjældent at blive en del af de vaner og rutiner, der skaber et fælles ansvar.

"Det sker jo ikke for os"-mentalitet

Når sikkerhed føles som noget, der kun gælder andre – store virksomheder eller offentlige institutioner – bliver det ikke prioriteret. Det giver en falsk tryghed og gør det sværere at få medarbejderne til at tage små advarsler alvorligt.

Lav arbejdsglæde og manglende ejerskab

Medarbejdere, der ikke føler sig motiverede, eller som ikke føler et ansvar for virksomhedens værdier, er mindre tilbøjelige til at følge retningslinjer. Når man ikke føler sig som en del af fællesskabet, bliver det også sværere at tage ansvar for sikkerheden.

Alt det modsatte af de nævnte eksempler er selvfølgelig med til at styrke sikkerhedskulturen. Når ledelsen går forrest, nye medarbejdere bliver godt klædt på, reglerne er til at forstå, og der er balance mellem effektivitet og ansvar – så er man godt på vej mod en stærk sikkerhedskultur, hvor alle bidrager aktivt.

Nu har du fået indsigt i, hvorfor en sund og stærk IT-sikkerhedskultur er afgørende for enhver arbejdsplads.

Du har også fået et billede af, hvordan en stærk kultur ser ud – og hvordan en svag kultur kan komme til udtryk.
Det kan være en god anledning til at reflektere over, hvor din egen arbejdsplads befinder sig på den skala.

Vi har gennemgået nogle af de typiske faktorer, der kan svække en sikkerhedskultur, og du har forstået, hvordan det modsatte af disse kan være med til at styrke den.

I det næste afsnit dykker vi ned i konkrete og anvendelige råd til, hvordan du – uanset din rolle i organisationen – kan være med til at løfte sikkerhedskulturen og skabe et tryggere digitalt arbejdsmiljø.

Praktiske råd til at styrke din sikkerhedskultur

En stærk sikkerhedskultur skabes ikke fra den ene dag til den anden.
Det er en løbende proces, hvor både små og større tiltag er med til at forme adfærden i organisationen. De følgende anbefalinger er baseret på både praktiske erfaringer og anerkendte metoder inden for IT-sikkerhed – og er med fuldt overlæg inspireret af Cyberpilot, der er blandt de førende eksperter i awareness-træning og medarbejderuddannelse inden for cybersikkerhed.

Disse tiltag er et oplagt udgangspunkt for dig, der vil styrke den sikkerhedsmæssige adfærd i din virksomhed.

Kommunikér klart om IT-sikkerhed

Det hele starter med, at medarbejderne ved, hvad der forventes af dem. Mange virksomheder fejler ved at lave alt for lange og tekniske politikker, som ingen læser. Gør det i stedet let og forståeligt – skriv kort, konkret og i øjenhøjde. Politikkerne bør introduceres allerede ved onboarding og gerne være koblet til obligatorisk awareness-træning.

Etabler en tydelig rapporteringsvej

Medarbejderne skal vide, hvor og hvordan de rapporterer sikkerhedshændelser. Hav en simpel og kendt proces, og test løbende om den virker i praksis – fx med simulerede phishing-mails. Det handler ikke kun om at kende proceduren, men om at træne en kultur, hvor det er naturligt at dele og handle på sikkerhedstrusler.

Involver ledelsen

Ledelsen spiller en afgørende rolle i at sætte tonen. Når topledere prioriterer IT-sikkerhed og deltager i awareness-træning på lige fod med resten af organisationen, bliver de rollemodeller, som smitter af på medarbejdernes adfærd.

Mål udviklingen

For at se om indsatsen virker, er det nødvendigt at måle. Hvor mange gennemfører træning? Hvor hurtigt gør de det? Skal der mange påmindelser til? Brug dataen til at justere og forbedre løbende.

Gør det personligt

IT-sikkerhed vedkommer alle – ikke kun IT-afdelingen. Derfor er det vigtigt at vise medarbejderne, hvilken rolle de spiller. Simulerede phishing-mails er en effektiv metode til at synliggøre, at alle kan blive ramt og har et ansvar.

Anerkend god sikkerhedsadfærd

Positiv forstærkning virker. Når du fremhæver teams eller enkeltpersoner, der udviser god sikkerhedsadfærd, skaber du rollemodeller og motiverer andre. Anerkendelse – både social og måske i form af små incitamenter – kan gøre en stor forskel.

Gør det til en del af hverdagen

Sikkerhed skal ikke være noget, man "tager kursus i". Det skal leve i hverdagen. Brug fx plakater, små reminders, og korte læringsforløb – og varier gerne medieformerne for at fastholde interessen.

Tænk langsigtet

En stærk sikkerhedskultur skabes og vedligeholdes over tid. Det kræver kontinuitet. Planlæg regelmæssige awareness-aktiviteter og hold fokus ved lige – fx med korte læringsmoduler hver anden måned og små påmindelser ind imellem.

Lad os tage dialogen videre –
vi hører gerne fra dig.