6 tips

til hvordan forebygge og sikre bedriften din mot dataangrep

evelon

Den teknologiske utviklingen er stadig i bevegelse og måten vi jobber på endres i takt med alt som skjer i den digitale verden. Norge er i verdenstoppen når det gjelder digitalisering, noe som har gitt resultater innenfor innovasjon og utvikling.

I takt med den teknologiske utviklingen møter alle som benytter seg av skybaserte digitale løsninger og tjenester også en rekke nye utfordringer og krav i forhold til sikkerhet. Flertallet av norske virksomheter benytter seg av tjenester i skyen. Skybaserte tjenester gir muligheter for bedre arbeidsflyt, men vi stiller oss også mer åpne og sårbare for cyberkriminalitet dersom vi ikke sikrer oss godt nok.

evelon

Hvorfor skybaserte løsninger?

Ved bruk av skytjenester trenger du verken å tenke på nedetid eller vedlikehold, da de er bygget opp slik at informasjon og applikasjoner i skyen er fordelt på flere servere som fungerer som en. Skulle en av serverne slutte å fungere, vil en annen ta over. Der tradisjonelle IT-systemer har begrenset kapasitet, er den nærmest uendelig i skyen.

Hvordan jobbe effektivt, skape lønnsomhet, og samtidig være trygg i skyen?

Enhver virksomhet er opptatt av vekst, og det er som kjent mange faktorer som spiller inn for at en virksomhet skal være lønnsom. En av disse er selskapets infrastruktur. Har du et godt verktøy for samhandling, informasjonsflyt og sikring av data og nettverk, er du på god vei. Da kan du spare både tid og ressurser. Arbeidsoppgaver, som for eksempel omfatter administrasjon, personalsaker eller utforming av en Powerpoint, er lett tilgjengelig for alle som skal ha tilgang. All utveksling og deling av data skjer på en sikrere måte gjennom stadig oppdaterte verktøy

evelon

Hvordan kan man være sikker på at bedriften og de ansatte er sikret nok?

51% av bedrifter som benytter et styringssystem oppdager hendelser i større grad ved intern sikkerhetsmonitorering. Virksomheter som sikrer informasjonsflyten sin gjennom styringssystemer, opplever at tilfeldigheter og uflaks i mindre grad er årsak til uheldige hendelser.

Bedriften er med andre ord sikrere med et styringssystem eller -verktøy, som skal bidra til at bedriften unngår ondsinnede angrep med ulike innfallsvinkler, enn uten. Det er mange eksempler på gode styringsverktøy. Microsoft 365 er et av dem, som gjør det mulig for alle å være kreative og jobbe sammen på en sikker måte.

> Vårt viktigste råd er å sørge for god intern opplæring slik at brukerne er bevisste på hvordan de håndterer data internt og eksternt i bedriften og at de er oppmerksomme på "unormaliteter"
>
> — Andreas Hornberg, Senior Kunderådgiver

evelon

Trender i sikkerhet følger dagens trusselbilde

Det arbeides kontinuerlig med utvikling av nye metoder som vil avdekke cyberkriminalitet i tidlig fase, og det er i stor grad de cyberkriminelle som styrer utviklingen av gode sikkerhetsløsninger. De ligger som regel et halvt hode foran, og blir stadig mer oppfinnsomme og profesjonelle i utføringen av sine digitale kriminelle handlinger, enten det er via skyen eller lokale servere eller enheter. For å bekjempe angrepene må vi følge opp de kriminelle trendene med kunnskap, forebyggende tiltak og smarte løsninger, som oppdager og avslører ondsinnede angrep i våre datasystemer.

evelon

1. Phishing

Nettfiske er et problem som bedrifter og deres ansatte bør ha fokus på. Dette er målrettede angrep gjennom infiserte e-poster, hvor en prøver å få deg til å oppgi brukernavn og passord. Slik kommer hackeren inn i systemer som kan misbrukes. Det er viktig å være bevisst på e-postsikkerhet, da angriperne blir stadig mer utspekulerte og vanskeligere å oppdage.

Direktørsvindel spinner ut fra phishing, hvor hensikten er å få deg til å utføre en handling via e-posten din. Svindlerne kan bruke tid inne i systemet og kartlegge roller og relasjoner i bedriften før de angriper på en sofistikert måte. Et eksempel kan være å sende svært troverdige e-poster i ditt navn. Denne typen svindel er vanskelig å oppdage eller å lage tekniske barrierer mot.

Tips

Foruten å være i besittelse av et godt styrings- og sikkerhetssystem som kan oppdage og luke ut mistenkelige e-poster – både med og uten vedlegg – gjelder det å være oppmerksom. Får du en e-post fra noen som ber deg om å oppgi sensitiv informasjon, bør det ringe noen varselklokker. Da kan det være bra å benytte seg av tofaktorautentisering ring, som fungerer omtrent som BankID. Med tofaktorautentisering har du en sikrere støttefunksjon som gjør at du ikke trenger å forholde deg til alle forsøk på svindel.

En løsning kan være å benytte seg av Advanced Threat Protection (ATP), som gir utvidet beskyttelse av bedriftens e-post mot usikre vedlegg og skadelige koblinger. ATP sørger for at:

- Mistenkelig innhold går gjennom en sanntidsanalyse for søk etter skadelig programvare.

- Maskinlæringsteknologi benyttes for å vurdere innholdet for mistenkelig aktivitet, resultatet er en innboks fri for skadelig programvare

- Alt innhold blir sendt via e-post blir skannet, nettadresser undersøkes i sanntid. Dersom en kobling er skadelig advares brukeren mot å besøke

2. Ransomware

Også kjent som løsepengevirus eller krypteringsvirus. Dette skjer ved at cyberkriminelle saboterer og låser av systemet ditt og krever løsepenger for å gi tilbake data. Aktørene har blitt flinkere og oppdaterer kontinuerlig sine verktøy og teknikker for å trenge inn i dine datasystemer.

Tips

Sørg for at enheter som disker og liknende ikke er tilkoblet datamaskinen din til enhver tid, siden denne formen for virus kan spre seg til disse. Sørg for å holde datamaskinens operativsystem og programvare oppdatert. Har du Windows 10, har du en innebygget beskyttelse mot ransomeware i ulike former, som kalles Controlled Folder Access. Du må selv aktivere funksjonen og spesifisere hvilke mapper uautoriserte programmer skal få tilgang til, i tillegg til standarden som er Dokumenter, Bilder og Skrivebord.

En løsning for mer beskyttelse kan være å sette opp betinget tilgang, hvor bedriftens data kan begrenses til å kun behandles i administrerte applikasjoner som bedriften har kontroll over. På den måten kan man forhindre lekkasje av data til for eksempel privat OneDrive, Dropbox eller andre systemer som bedriften derimot ikke har kontroll over.

evelon

3. Kompromittering av utdaterte webserverinstallasjoner

Dette er en form for angrep som ofte rammer mindre bedrifter med begrensede IT-ressurser. Flere av disse har sårbare versjoner av ulike programvarer, og implementasjoner av systemer hvor funksjoner eller programmer har svakheter i design eller tjeneste. De kan også være feilkonfigurert. Det som skjer er at angriperne utnytter svakhetene til å komme til servere, som igjen blir brukt som mellomledd i nye angrep mot nye mål.

Tips

Det er både sikrere og mer lønnsomt å kontinuerlig oppgradere systemene sine for å unngå å være utsatt for kjente sikkerhetshull. Løsningen kan være å bruke en IT-leverandør som drifter ditt IT-miljø og passer på for deg.

evelon

4. Angrep på verdikjeden i bedriften

Stadig nye angrep via leverandører baner vei inn i verdikjeden i bedriften. Har bedriften et svakt ledd i verdikjeden sin, er det stadig flere som velger denne måten å angripe bedriften på.

Tips

Skulle uhellet være ute, er det av stor betydning at bedriften har gode rutiner for å håndtere og gjenopprette sitt IT-miljø. En sertifisert aktør innen IT-sikkerhet og – systemer, som er både kjent og pålitelig, vil kunne være til stor hjelp ved å bistå bedriften med sine tjenester.

Detaljert rapportering og meldingssporing, samt intelligent beskyttelse og sikkerhetsanalyser kan være løsningen her. Du får innsikt i hvem i organisasjonen din som er typiske mål for angrep, og hvilken type angrep dere utsettes for. Rapportering og meldingssporing gjør det mulig for bedriften å undersøke meldinger som er blokkert på grunn av ukjent virus eller skadelig programvare.

Med intelligent beskyttelse og sikkerhetsanalyser får du større mulighet til å oppdage en kompromittert bruker og automatisk respondere på trusselen. Du vil også ha full kontroll med oversikt og sikkerhetsanalyse over alle data og applikasjoner som benyttes i bedriften. Power BI sørger for rapporter internt i bedriften.

evelon

5. Kontroll over mobile enheter

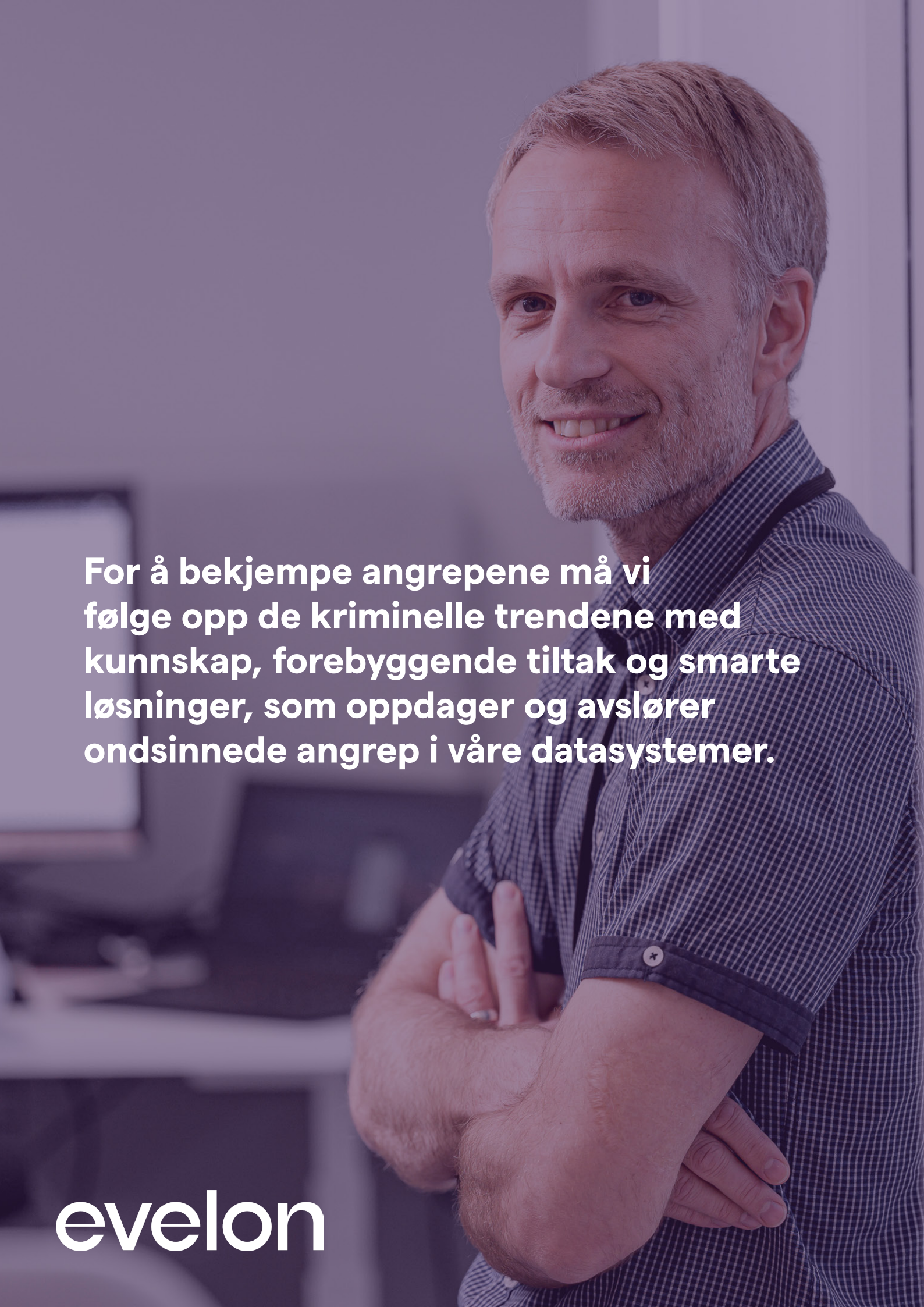
De fleste i dag har flere enheter som benyttes både i jobb og privat. Disse kan være svært sårbare for angrep hvis man ikke har sørget for tilstrekkelig enhetsikkerhet, på samme måte som på stasjonære enheter. Angrep mot mobile løsninger kan for eksempel være rettet mot betalingstjenester og andre tjenestetilbud, hvor malware har til hensikt å angripe for eksempel banker, bankansatte og nettbankkunder. Denne formen for kriminalitet er svært avansert og velorganisert, utøverne har store utviklingsressurser og stor infrastruktur med kompromitterte servere.

Tips

Det er viktig å ha kontroll på hvilke applikasjoner og tjenester du har lov til å benytte deg av i jobbsammenheng. Et klart skille mellom privat og jobb er essensielt for å sikre at ikke data havner feil. Derfor må man også ha kontroll på mobile enheter som man benytter seg av utenfor kontoret. Sentral administrasjon av operativsystem og applikasjoner vil høyst sannsynlig gi både økt effektivitet og bedre sikkerhet. En tjeneste som Mobile Device Management (MDM) er en enkel men nyttig form for administrasjon for integrering og styring av mobile enheter inkludert bærbare datamaskiner og nettbrett. Systemet segregerer i hovedsak bedriftens data, sikrer e-post og bedriftsdokumenter per enhet og håndhever bedriftens retningslinjer. Disse tjenestene kan avanseres med en EMM-løsning.

Her kan løsningen ligge i enhetsadministrasjon, et systemkrav om at brukernes enhet innrulleres og firmaet får kontroll over enheten, og at firmaets retningslinjer opprettholdes. Dette kalles Enterprise Mobility + Security, som er en enkel og effektiv administrasjon med moderne sikring av data og enheter i skyen. Blir for eksempel en enhet stjålet eller mistet, er det mulig å fjernslette alt på enheten.

evelon


For å bekjempe angrepene må vi følge opp de kriminelle trendene med kunnskap, forebyggende tiltak og smarte løsninger, som oppdager og avslører ondsinnede angrep i våre datasystemer.
evelon

6. Kryptojacking / Kryptomining

Dette er en form for datakriminalitet og type angrep som er fordoblet det siste året. Ondsinnede aktører jobber målrettet mot mottakelige maskiner med sårbare operativsystemer, for prosessorkraft for ulovlig utvinning. De kaprer med andre ord datamaskinen din – enten lokalt eller i nettleseren – og det kjøres et program (malware) som bruker datakraft til å utvinne kryptovaluta uten at du merker det. Kryptovaluta er enkelt forklart elektroniske penger – kanskje mest kjent som Bitcoin her til lands. En annen måte å utføre Kryptojacking på er å ramme skybaserte tjenester, der et nettverk med servere brukes til å behandle og lagre data, som igjen gir mer databehandlingskraft til selskaper som ikke har investert i ekstra maskinvare.

De som utsettes for kryptojacking kan merke det på høye strømregninger og langsommere ytelse i programmer/ maskinparken, eller at enheten blir varm og at viften for avkjøling øker kraftig.

Slike angrep ødelegger ikke filer men maskinen kan bli overopphetet og dermed ødelagt. For å unngå denne typen angrep er det viktig å oppdatere programvaren, for eksempel Windows, sørge for at du har et godt sikkerhetssystem som beskytter mot denne typen datakriminelle, samt forsikre deg om at filer du mottar kommer fra pålitelige kilder.
Du kan beskytte deg ved å;

- Aktivere Windows-sikkerhetsfunksjoner
- Holde alle programvarer oppdatert
- Være forsiktig med å åpne uventede vedlegg eller linker i e-post
- Holde deg til godkjente sider når du surfer på Internett
- Ikke bruke piratkopiert materiell
- Opprettholde gode sikkerhetskopier av dataene dine og teste dem regelmessig

evelon

Mer avanserte angrepsmetoder

Angriperne blir stadig mer sofistikerte i sine fremgangsmåter. Angrepene er innsiktsfulle og profesjonelle både i forhold til målet, med tanke på research over tid i forkant, og utførelse. Hvis vi tar phishing som et eksempel, er både utførelse i design, språk og tema svært profesjonelt og troverdig utført, og er vanskelig å avdekke før uhellet er ute

Hva kan vi gjøre på generelt grunnlag forebyggende eller unngå for stor skade?

Ha kontroll på infrastrukturen, altså virksomhetens data og tjenester. Sørg for sikker pålogging og hvem som har administrative privilegier og hensiktsmessig logging.

Det kan være smart å kjøpe IT-tjenester hos profesjonelle aktører, for lavere og mer forutsigbare kostnader og tilgjengelige tjenester.

Sørg for at den som skal bestille tjenester hos leverandør har god kompetanse og kan ta gode risikovurderinger for å kunne ta riktige beslutninger. Ikke være redd for å stille krav til IT-løsningen og leverandøren. Sørg også for beskyttelse av og kontroll på ansattes enheter og filer.

NorSIS anbefaler følgende tiltak

Grundig opplæring og trening i sikkerhet vil både forebygge hendelser og sørge for at konsekvensene blir mindre når hendelsen er et faktum. NorSIS** anbefaler følgene tiltak for å sikre din bedrift.

- Sørg for at medarbeiderne får opplæring i virksomhetens sikkerhetsrutiner med et spesielt fokus på å motstå sosial manipulering og svindel.

- Styrk medarbeideres sikkerhetskunnskap, ved å gi dem innsikt i trusselbildet og hvordan de ved å følge virksomhetens sikkerhetsprosesser kan minske faren for uønskede hendelser.

- Kartlegg virksomhetens digitale sikkerhetskultur for å avdekke om det er behov for å igangsette tiltak.

- Økonomimedarbeidere bør få opplæring om direktørsvindel, og virksomheten bør innføre rutiner rundt overføringer av større beløp som gjør det vanskeligere for direktørsvindlere å lykkes.

Kontakt oss

Ikke nøl med å ta kontakt med oss dersom det er noe du lurer på. Hvis du booker et møte med oss gir vi deg kostnadsfri rådgivning på hvordan du kan få mer ut av ditt Microsoft 365 abonnement.

Abonner på fagbloggen

Book et møte

www.evelon.no
21 41 50 00
salg@evelon.no

Kilder

***Næringslivets sikkerhetsråd:** Mørketallsundersøkelsen – Næringslivets Sikkerhetsråd (nsr-org.no)

****Norsk senter for informasjonssikring:** https://norsis.no/

evelon