Buckle up!

Er bedriften din rigget for fremtidens digitale sikkerhet?

Telia Trend report
First edition

Telia Company

Innhold

1. utgave september 2024

Sikkerhet starter med menneskene

I takt med at digitaliseringen skyter fart, blir samfunnet også mer sårbart for digitale trusler. Hackerangrep og annen cyber-kriminalitet øker for hvert minutt som går, og mange bedrifter henger etter.

Digital sikkerhet er en kompleks og kostbar problematikk, men ikke la det stoppe dere fra å komme i gang. Å styrke digital motstandskraft vil forebygge kostbar nedetid forårsaket av avanserte cyberangrep, og reduserer risikoen for databrudd som kan skade både selskapet og de ansatte. Faktum er at beskyttelse av folks data og privatliv bygger tillit, noe som er særdeles viktig i en tid da ordet personvern er på alles lepper. Robust sikkerhet fører med seg betydelige gevinster, og dette gjelder overalt og innen enhver sektor. I en situasjon der digital sikkerhet er viktigere enn noensinne, er det innlysende at emnet fortjener vår oppmerksomhet.

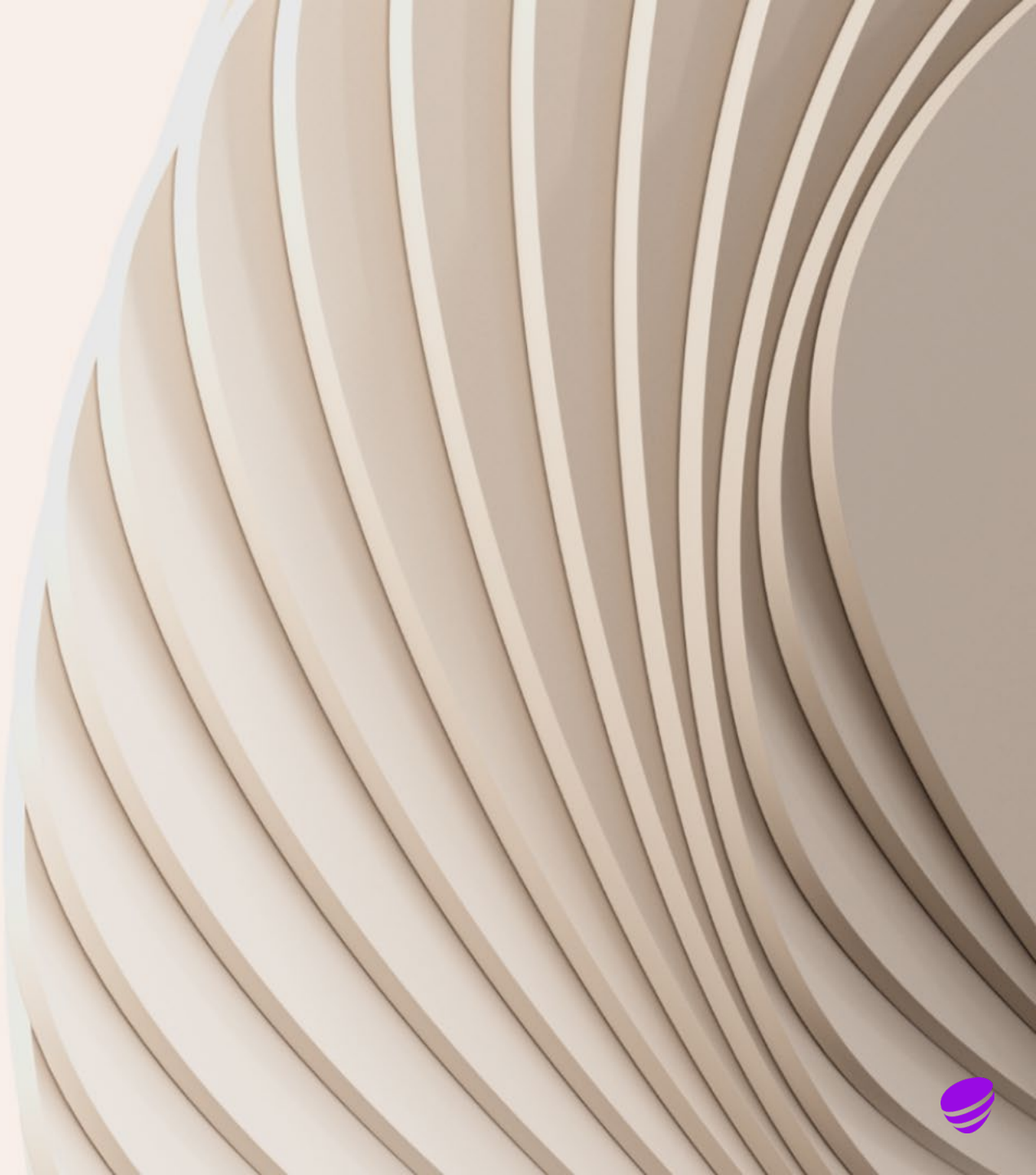
Som en ledende aktør innen digital sikkerhet vet vi i Telia hva som skal til for å bygge motstandskraft. Teknologi og prosesser er viktige, men vi har erfart at mennesker er et kritisk punkt. Mennesker er enkle å hacke. Hvis du ikke har godt opplærte og motiverte medarbeidere i ryggen, spiller det mindre rolle hvor mye du investerer i verktøy og teknologi.

Denne rapporten utforsker den avgjørende rollen menneskers adferd og emosjoner spiller for digital motstandskraft. Gjennom vårt samarbeid med sikkerhetseksperter, kunder og bransjeledere har vi fått dypere forståelse av noen av utfordringene organisasjoner står overfor i dag, og har utviklet praktiske råd for hvordan du kan overvinne dem. Nå deler vi innsiktene for å styrke bevisstheten, stimulere til samtaler og bidra til den løpende innsatsen for sammen å skape en mer velfungerende databasert hverdag – både i arbeidslivet og ellers.

Vi håper å kunne inspirere bedrifter overalt til å ta de nødvendige grepene.

02

Sett i perspektiv



Vår tids sikkerhetsbelte

I 1959 ble det første trepunkts sikkerhetsbeltet lansert, med potensial til å forbedre overlevelsesraten etter bilulykker dramatisk. Til tross for holdningskampanjer og bilindustriens raske implementering, var folk flest sene med å ta de nye sikkerhetbeltene i bruk. Hvorfor? Det er utfordrende å endre gamle vaner, til og med når det er vår egen overlevelse som står på spill.

I dagens heldigitaliserte verden står vi overfor trusler som er langt mer komplekse og abstrakte enn trafikkulykker. Og som tilfellet var med biler og sikkerhetsbelter, blir den digitale sikkerheten ofte ansett som sekundær eller er noe man først tenker på i etterkant. Vi har vært for naive når vi har tatt hensyn til sikkerhetsgrensene på de digitale motorveiene.

Den langsomme, men etter hvert omfattende innføringen av sikkerhetsbeltet, er en tankevekkende påminnelse om noen få elementære sannheter vedrørende innovasjon, mennesker og sikkerhet:

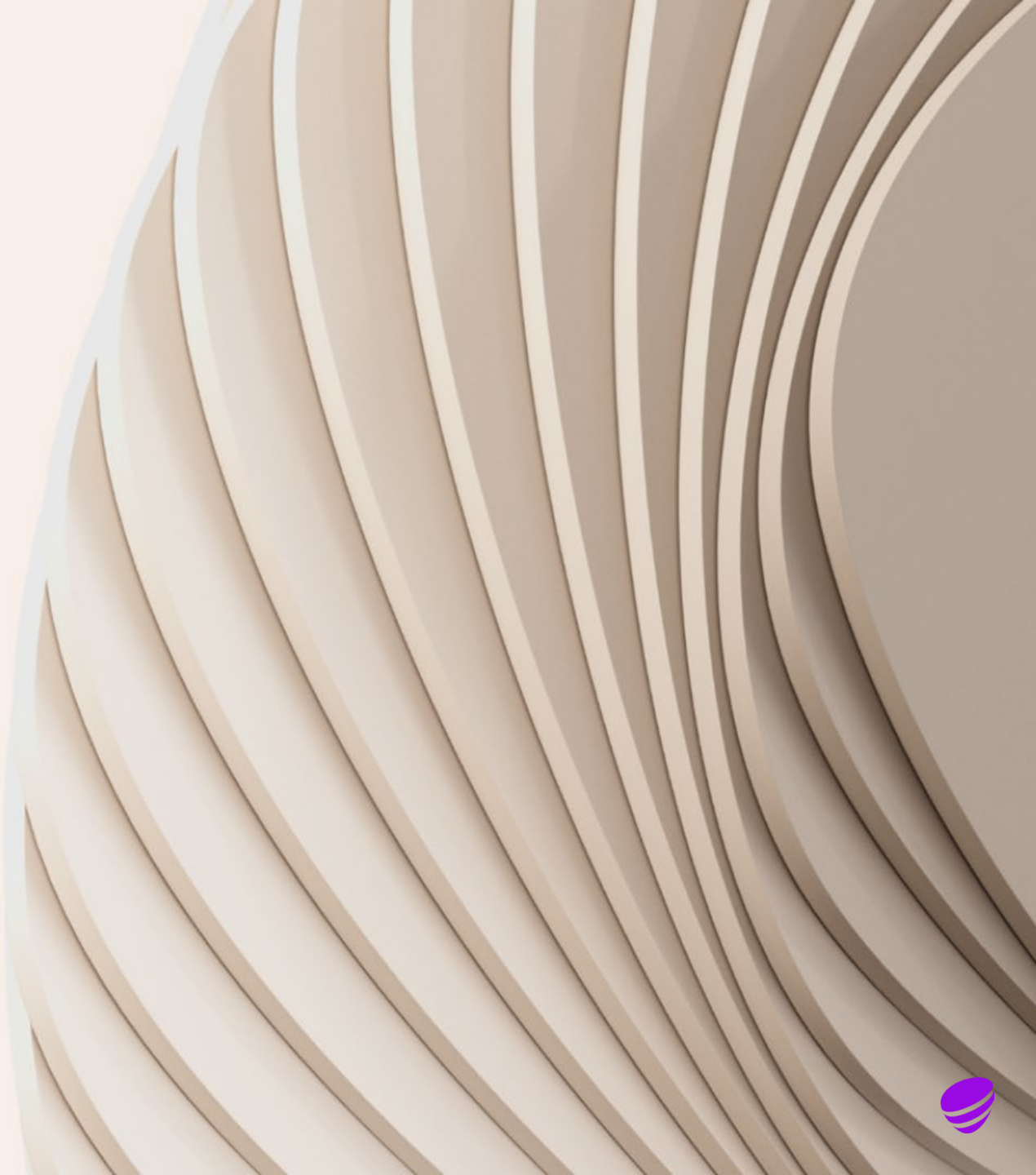
- I den svært konkurransedrevne utviklingen og spredningen av ny, banebrytende og ofte dårlig forstått teknologi, er sikkerhet sjelden en topprioritet for noen av de involverte – dersom den prioriteres i det hele tatt. Først gradvis, etter hvert som ulempene ved den nye teknologien begynner å bli åpenbare for alle, får sikkerheten den oppmerksomheten den hadde fortjent i utgangspunktet.
- Selv når sikkerhetstiltak er på plass, er det ingen garanti for at alle vil etterleve dem på en måte som står i et rimelig forhold til risikoene teknologien fører med seg.
- Sikkerhet som et konsept og en praksis er ofte lite håndgripelig, og må forenkles og konkretiseres før vi som enkeltmennesker begynner å se, forstå, bry oss og handle.

I motsetning til i trafikken er den digitale trusselen forsettlig: Cyberkriminelle retter seg aktivt og med økende effektivitet mot en stadig voksende gruppe av ofre. Og nå som vi er på full fart inn i det nye og ukjente territoriet kunstig intelligens, trenger vi ikke bare å ha de riktige sikkerhetsløsningene på plass, men også å lære hvordan vi spenner oss fast.

Dette er vår tids sikkerhetsbelte-øyeblikk.

3

Metodikk



Metodikk

Formålet med rapporten er å gi en skisse av hvordan fremtiden innen digital sikkerhet vil bli for bedrifter. Rapporten baserer seg på flere ulike forskningsmetoder, som kombinerer primære, kvantitative og kvalitative data fra mange kilder. Forskningen ble utført våren 2024.

- **13 dybdeintervjuer** med beslutningstakere innen sikkerhet (f.eks. CISO, CIO) i store foretak og organisasjoner i ulike bransjer i Telias viktigste markeder i Norden og Baltikum.
- **9 dybdeintervjuer** med anerkjente eksperter på cybersikkerhet og digital sikkerhet, samt profilerte eksperter hos Telia (vist til høyre).
- **Gruppesamtaler med eksperter**, som samlet over 15 tverrfunksjonelle spesialister fra den bredere Telia-organisasjonen, herunder Risk, Strategy, Human Resources, Innovation, Communication og Cybersecurity (se vedlegg).
- **Data og innsikt** fra ledende bransjerapporter og -artikler
- **Data fra Telias Digital Index 2024**, som henter informasjon fra 1152 organisasjoner av alle størrelser. TDI er en årlig spørreundersøkelse som følger svenske selskapers digitale utvikling.

Konsulterte eksperter

En spesiell takk til disse ekspertene, som bidro med verdifulle og grundige perspektiver og innsikt til denne rapporten.

Anne-Marie Eklund Löwinder

CEO Amelsec og Cyber Security Expert

Mehis Hakkaja

CEO og eier av Clarified Security OÜ

Åke Holmgren

Head of Cybersecurity, MSB – Myndigheten för samhällsskydd och beredskap i Sverige

Pontus Johnson

Professor KTH og direktør i Center Cyber Defense and Information Security

Niclas Jalvinger

CISO/CSO, Telia

Michael Mothander

Cyber Security Expert, Telia

Malin Fransén Kronberg

Head of Security, Telia

Simon Binder

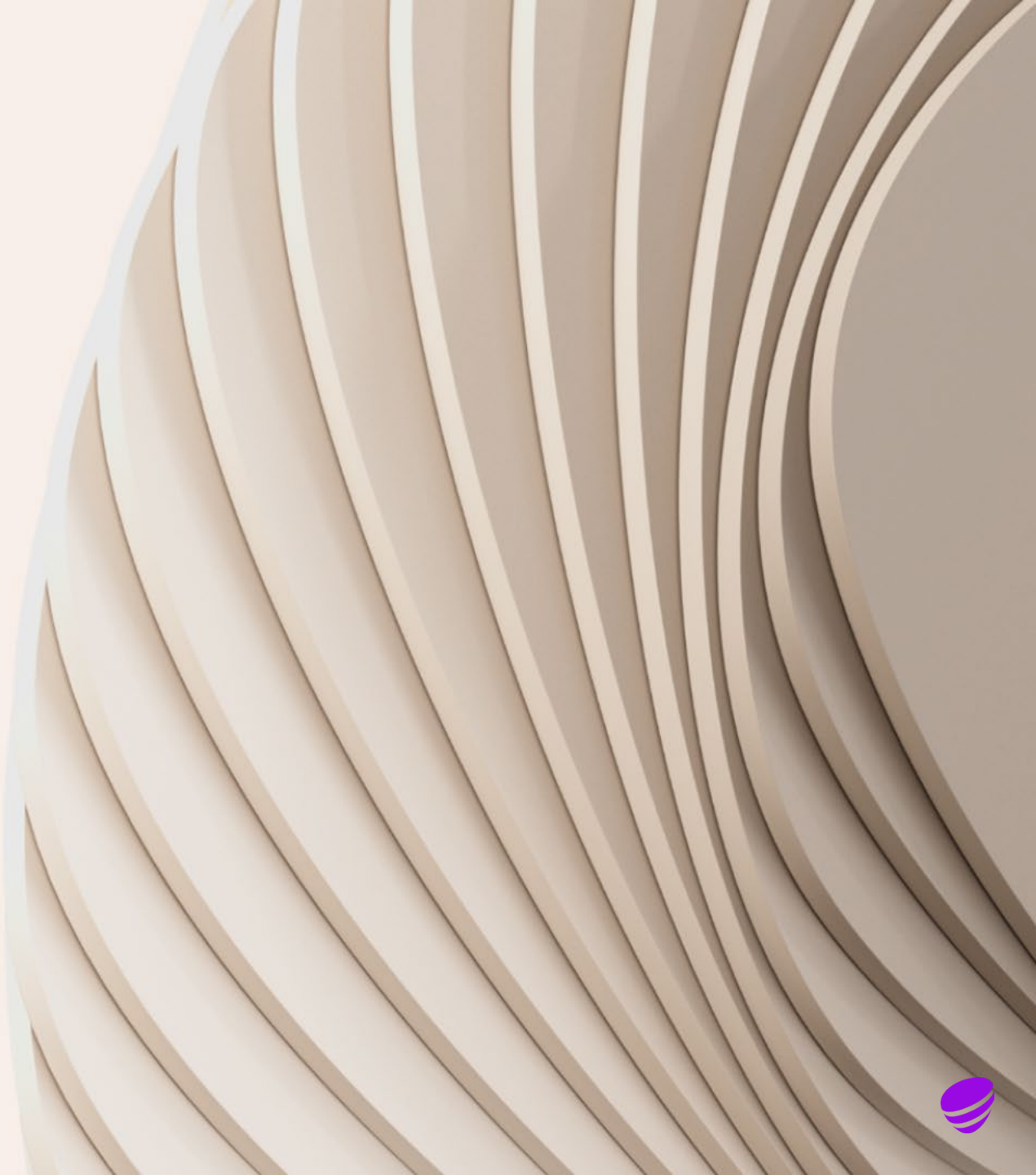
Cyber Security Expert

Mats Mägiste

Security Infrastructure Expert, Telia

4

Status for digital sikkerhet



En tredemølle – som bare går raskere og raskere

91 %

av organisasjonene rapporterte minst én cyberhendelse eller ett databrudd i 2022
Kilde: Deloitte, Global Future Cyber Security 2023

+466 %

økning i DDoS-angrep i Sverige i K1 2024 sammenlignet med K1 2023
Kilde: Cloudflare DDoS threat report, 2024

En kamp som omfatter mer enn konkurranse

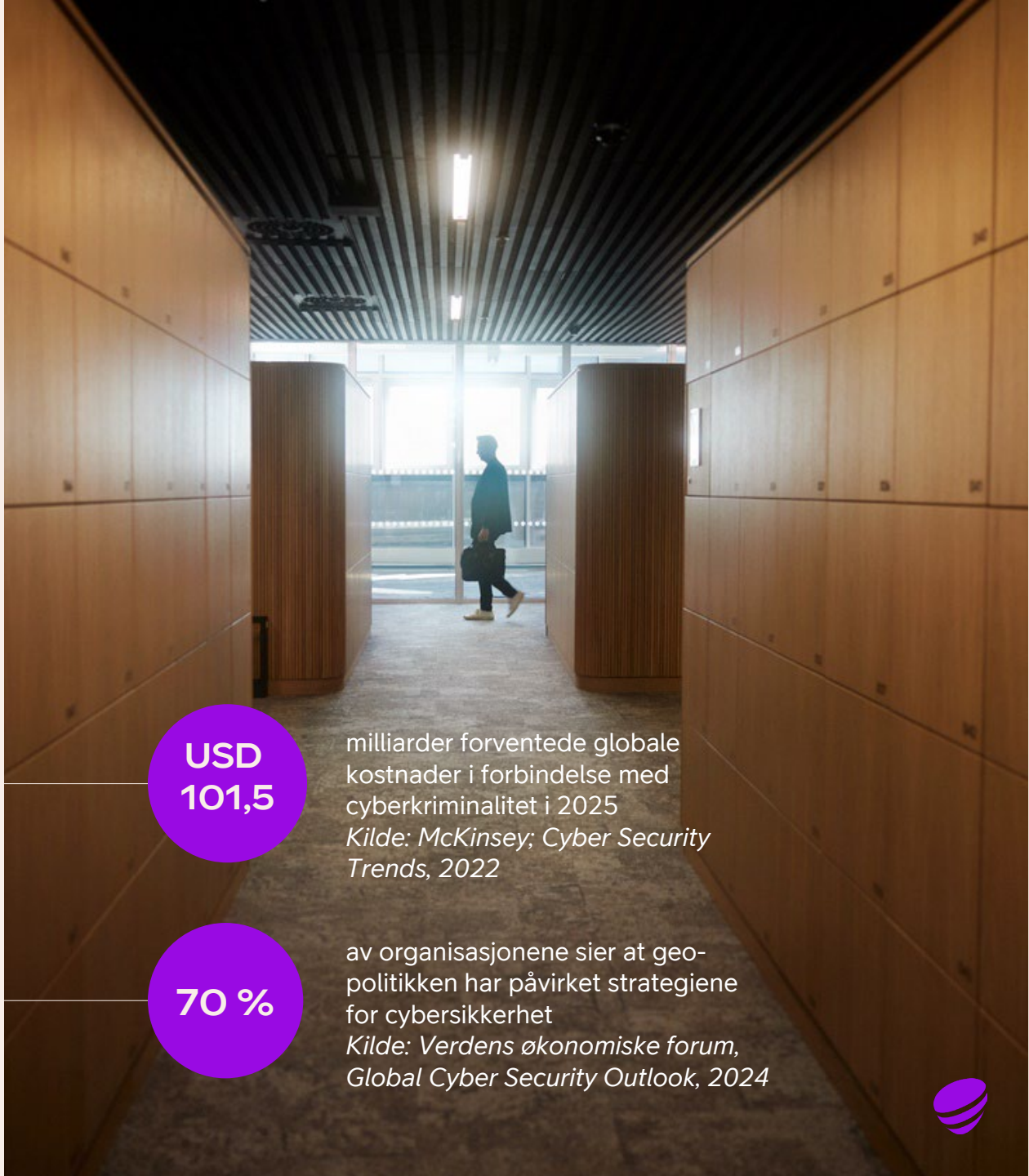
I naturen kan den pågående evolusjonen sammenlignes med et evigvarende våpenkappløp mellom konkurrerende arter. Tilpass deg eller dø. For virksomheter har dette våpenkappløpet historisk sett handlet om å tilpasse seg eller skape nye markeder. Gradvis har det imidlertid utviklet seg en eksistensiell trussel som ikke følger spillereglene for vanlig markedskonkurranse.

I dag blir overlevelsen til store og små selskaper over hele verden truet av digitale trusselaktører – ikke ulikt invaderende arter i økosystemer – uansett hvor konkurransedyktige de er i markedet. Når vi så legger til den akselererende endringshastigheten, blir det tydelig at kampen for å unngå utryddelse vil bli enda mer intens i det kommende tiåret.

Sammenligningen med et våpenkappløp er bare en analogi, men den gir oss en nyttig innsikt: I likhet med for eksempel fysisk form, er ikke sikkerhet noen endestasjon. Man *oppnår* aldri noen total sikkerhet, bare løpende fremgang og tilpasning. Det faktum at vi brukte sikkerhetsbelte da vi kjørte bil i går, betyr ikke at vi vil være riktig fastspent i dag.

«Det er grunn til å anta at du kommer til å bli angrepet.»

CISO – global maskinvareprodusent



USD 101,5

milliarder forventede globale kostnader i forbindelse med cyberkriminalitet i 2025
Kilde: McKinsey; Cyber Security Trends, 2022

70 %

av organisasjonene sier at geo-politikken har påvirket strategiene for cybersikkerhet
Kilde: Verdens økonomiske forum, Global Cyber Security Outlook, 2024

Sikkerhetsgapet i Norden og Baltikum

Gjennom de siste tiårene har den digitale transformasjonen endret de fleste organisasjoner fundamentalt. Selv om Norden og de baltiske landene var tidlig ute med å ta digital teknologi i bruk, har sikkerhetsarbeidet ofte ikke holdt tritt. Historisk høye nivåer av tillit* og den relative roen gjennom de foregående tiårene, har etterlatt oss sårbare overfor et trussellandskap i hurtig utvikling.

I tillegg til vår godtroende fortid er en viss treghet også en medvirkende faktor, ikke minst i større og mer tradisjonelle organisasjoner. Det tar tid å legge vekk gamle vaner og etablere en ny sikkerhetstenkning.

Dette sikkerhetsgapet medfører betydelige utfordringer for organisasjoner som plutselig befinner seg i en helt annen verden enn tidligere, og nå ikke er tilstrekkelig forberedt på å forsvare seg mot og håndtere gryende trusler. Som tidligere direktør i FBI, Robert Mueller, har formulert det: *«Det finnes bare to typer selskaper – de som har blitt hacket, og de som kommer til å bli det.»*

Statusen for organisasjoners sikkerhet i dag er fragmentert. En organisasjons beredskap i møte med trusler avhenger i stor grad av nivået av digital sikkerhetsmodenhet, som den har vært i stand til å utvikle parallelt med sin digitale transformasjon. Selskaper som er etablert og bygget opp i den digitale tidsalderen, er naturlig nok bedre posisjonert til å takle fremtidige utfordringer, uansett hvor store eller små de er.

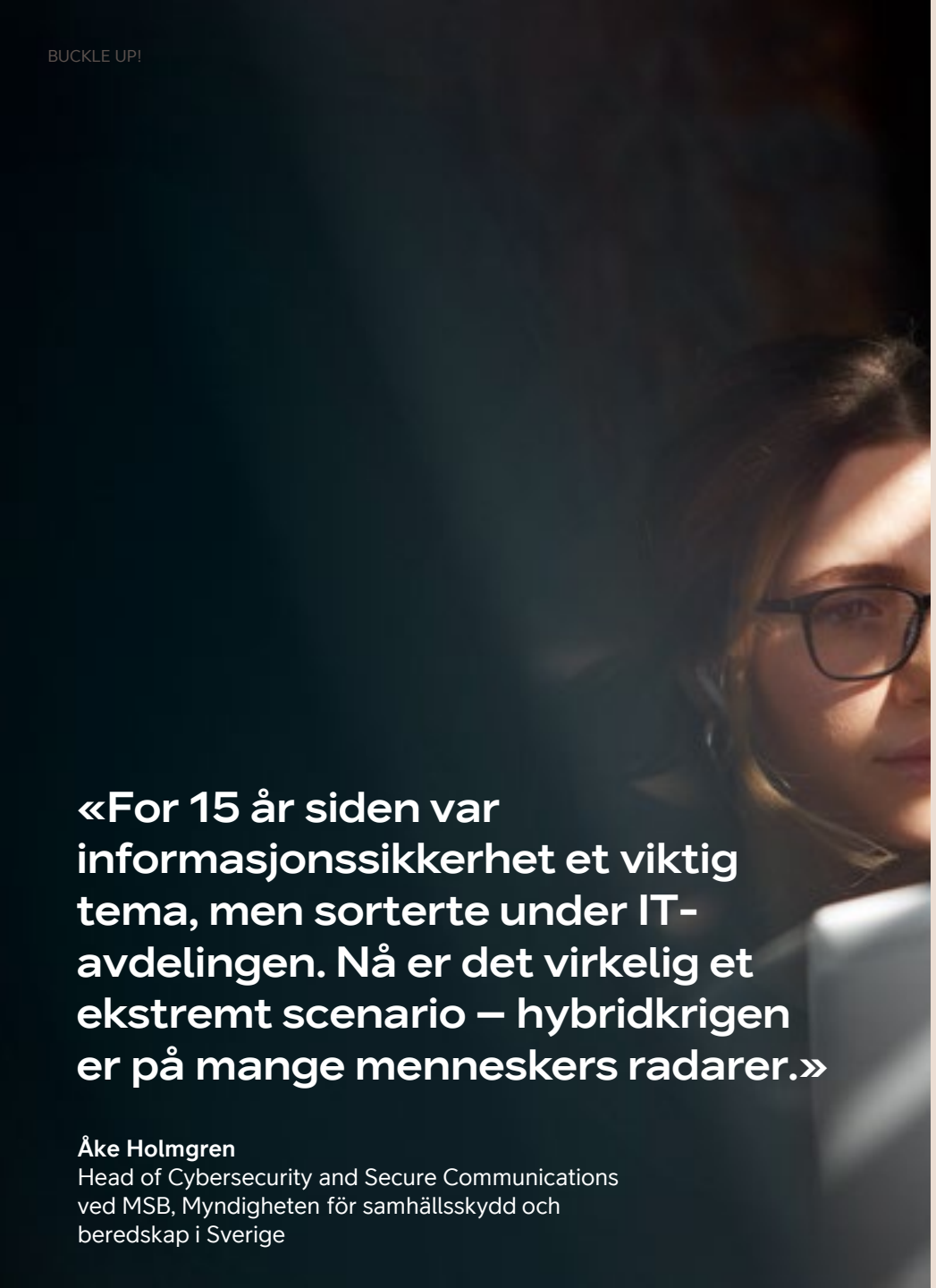
* Spesielt i Norden: Finland (78 %) og Sverige (68 %) er blant de landene i Europa der tilliten til myndighetene er høyest. *Kilde: OECD*

Kun 3 %

av offentlige instanser i Sverige tilfredsstiller kravene til cybersikkerhet i 2024
Kilde: MSB

«Selskaper trenger å gjøre mer. Nå. Det må bygges opp kunnskap i ledergruppen og styret. Problemet er nå altfor stort til bare å overlates til IT-avdelingen.»

Pontus Johnson,
professor ved Kungliga Tekniska högskolan (KTH) og direktør i Center for Cyber Defense and Information Security



«For 15 år siden var informasjonssikkerhet et viktig tema, men sorterte under IT-avdelingen. Nå er det virkelig et ekstremt scenario – hybridkrigen er på mange menneskers radarer.»

Åke Holmgren
Head of Cybersecurity and Secure Communications ved MSB, Myndigheten för samhällsskydd och beredskap i Sverige

Økende bekymring

2/3

sikkerhets-fagfolk i store selskaper bekymrer seg for cyberangrep
Kilde: Telia Digital Index 2024

Veksten i cyberkriminalitet begått av digitale leiesoldater og statsstøttede cyberterrorister, eskalerer voldsomt for tiden. Siden angrepene er større og mer omfattende enn før, kan de også forårsake mer skade enn noensinne. Organisasjoner som rammes av cyberangrep, kan fort befinne seg i den situasjon at de må klare seg uten kritiske systemer i uker eller til og med måneder.

Denne nye virkeligheten vekker betydelig uro blant sikkerhetsfagfolk: To av tre store selskaper bekymrer seg for potensielle angrep, en økning på 10 prosent siden 2023, ifølge Telias Digital Index 2024.

Simon Binder, Cyber Security Expert, har bitt seg merke i en holdningsendring fra selskapenes side: *«Store bedriftskunder er i dag mye mer bevisste på og nesten paranoide med hensyn til digital sikkerhet.»*

Organisasjoner later til å erkjenne at situasjonen er presserende, og investerer i robuste teknologiløsninger for å redusere sårbarheter i systemene sine. Likevel er det flere viktige utfordringer som må adresseres i tiden som kommer.

«Så lenge man kan tjene masse penger på veldig kort tid med lav risiko, kommer dette til å fortsette.»

Michael Mothander,
Cyber Security Expert, Telia

Sikkerhetsutfordringer organisasjoner står overfor i dag

01. Balansere investeringene i sikkerhet og teknologi

Fordelingen av investeringer mellom teknologi og digital sikkerhet er en løpende avveining. Det første har en tydelig, målbar effekt på forretningsvirksomheten, mens fordelene ved digital sikkerhet kan virke abstrakte med mindre en organisasjon har blitt direkte berørt. Så lenge sikkerhetsbudsjettet er innbakt i IT-budsjettet, er det en risiko for at midlene i økende grad vil gå til innføring av KI i stedet for å brukes til å styrke den digitale sikkerheten. Conor McGlynn, Director Group Head of Security Strategy and Transformation i Telia, sammenligner digital sikkerhet med forsikring: *«Sikkerhetsinvesteringer vil ikke oppfattes som verdifulle før noe skjer.»*

51 %

Andelen IT-sikkerhetssjefer som spår at det generelle IT-sikkerhets-budsjettet deres vil stagnere eller reduseres i 2024
Kilde: Pentera, The State of Pentesting, 2024

02. Forberede seg for det verste, ikke bare forebygge

Mange organisasjoner prioriterer forebygging og oppdagelse av uønskede hendelser, fremfor å forberede seg på det verste. Data fra Telia Digital Index 2024 viser at selskaper har flere løsninger for å identifisere, beskytte seg mot og oppdage trusler enn for gjenoppbygging og reparasjon etter et angrep. Nylige tall fra en Cisco-undersøkelse rettet mot 4700 sikkerhetsfagfolk, viser at organisasjoner som har vært utsatt for hendelser, er mer opptatt av å minimere tap og opprettholde forretningskontinuitet.

71 %

Andelen organisasjoner som mener at de ikke har løsninger på plass for gjenoppretting av tjenester etter et angrep
Kilde: Telia Digital Index 2024

03. Tiltrekke talentene og bygge kompetanse

Kompetansegapet er reelt: Bedrifter søker å tiltrekke og beholde IT-fagfolk, spesielt sikkerhetseksperter. Små og mellomstore selskaper står ofte helt uten intern sikkerhets-kompetanse, og må stole på tredjepartsleverandører og partnere. Denne mangelen på eksperter er en betydelig utfordring, særlig på kort sikt.

3,4 M

Nåværende estimert kompetansegap på cyber-sikkerhet globalt
Kilde: Allianz, Cyber security trends, 2023

04. Spredte sikkerhetstiltak gir dårlig oversikt

Digitaliseringsarbeidet foregår ofte i isolerte team i en organisasjon, noe som fører til spredte sikkerhetstiltak. Uten en felles helhetlig strategi blir den digitale sikkerheten ofte et sekundært element, i stedet for å tilrettelegge for forretningsdrift.

15 %

Andelen av organisasjonene som har nådd det høyeste nivået av modenhet (4), der cyber-sikkerhet er et prioritert perspektiv i hele virksomheten.
Kilde: Radar Cyber Maturity Index 2024.

Vent nå litt!

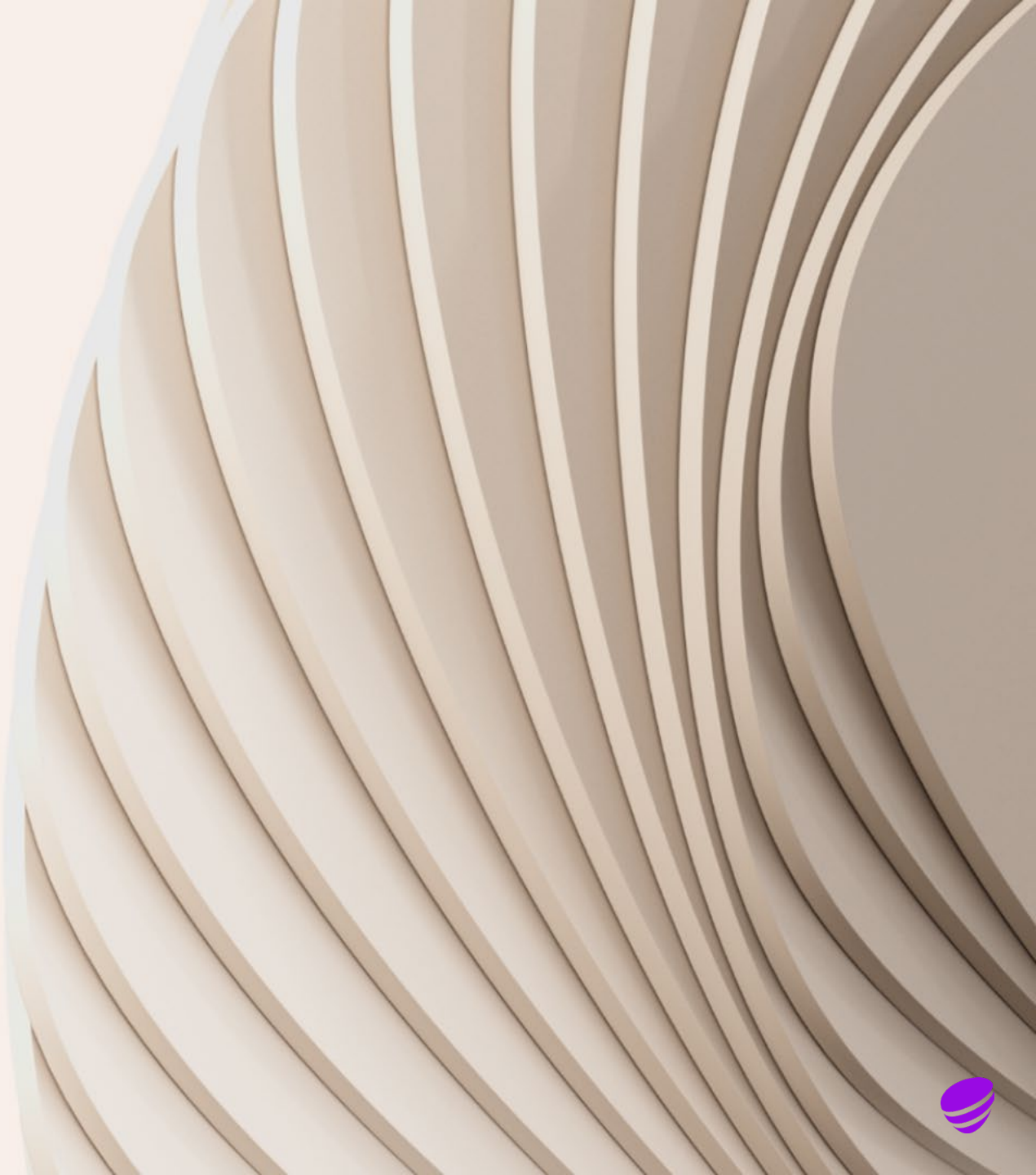
Du har kanskje lagt merke til at noe mangler i denne analysen: mennesker. Hold på den tanken et øyeblikk. La oss først ta en kort titt på hva organisasjoner prøver å oppnå ved å forbedre sikkerheten. Som tredemølle-metaforen lærte oss, er det bare de med digital motstandskraft som vil overleve. Så nøyaktig hva skal egentlig til?

«Det er ikke så usannsynlig at det vil stilles høyere krav til sikkerhet, spesielt med nye EU-regler. Seriøse organisasjoner vil foretrekke å gjøre forretninger med dem som har god nok sikkerhet.»

Åke Holmgren
Head of Cybersecurity and Secure Communications
ved MSB, Myndigheten för samhällsskydd och
beredskap i Sverige

05

Digital motstandskraft



96 %

Andel toppledere som mener at digital motstandskraft mot cyberangrep er svært viktig for virksomheten deres.
Kilde: Cisco, Security Outcomes Report, 2024

«Hvis et angrep skulle lykkes, er vi i stand til å reagere, avsløre angriperen og gjenopprette med minimal skade.»

IT-sikkerhetssjef – nordisk meieriforetak

NIST – et rammeverk for å bygge digital motstandskraft

1/5

Andel organisasjoner i gruppen «høy cyber-modenhet» *Kilde: Deloitte, Global Future of Cyber Survey 2023*

37 %

av bedriftene er trygge på at de kan stå støtt med digital motstandskraft under et verst tenkelig cyberangrep. *Kilde: Cisco, Security Outcomes Report, 2024*

Tilrettelegge for enkle løpende forbedringer

Å bygge digital motstandskraft krever strukturert arbeid og dedikerte ressurser. Heldigvis finnes det etablerte fremgangs-måter som kan hjelpe deg å komme i gang.

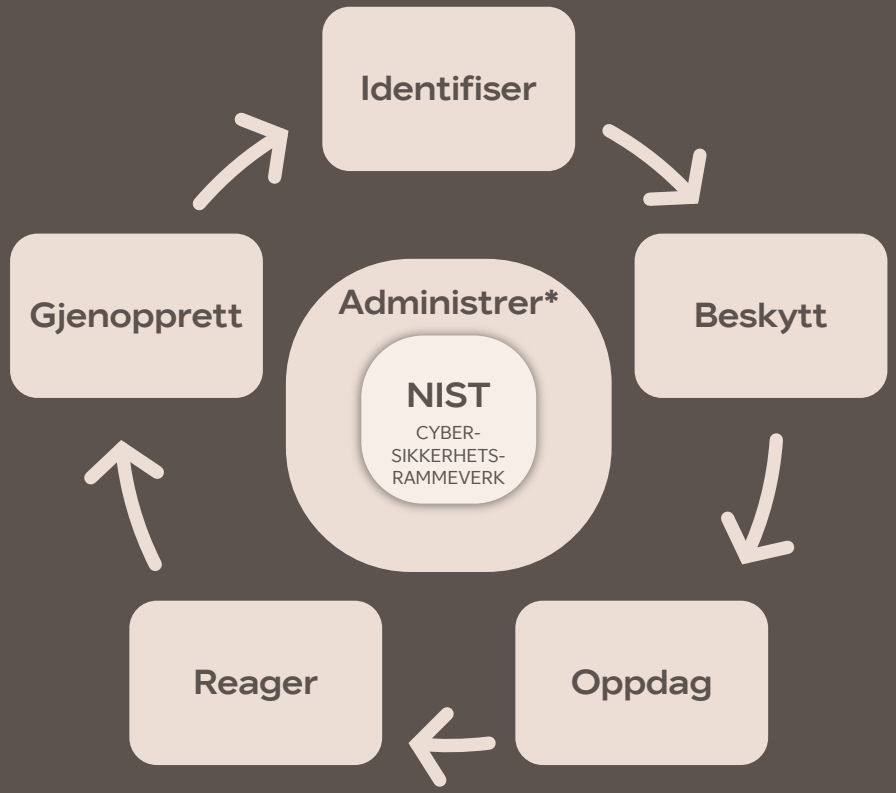
Det allment aksepterte cybersikkerhetsrammeverket NIST, definerer digital motstandskraft som *«evnen til å forutse, motstå, komme seg etter angrep. Og tilpasse seg negative tilstander, belastninger, angrep eller kompromitteringer av systemer som bruker eller aktiveres av cyberressurser».*

Denne definisjonen innebærer for det første at organisasjoner må konsentrere sikkerhetsarbeidet sitt – ikke bare om å beskytte seg mot og redusere effekten av angrep, men også om å kunne komme seg etter, lære fra og tilpasse seg uønskede hendelser som de eller andre utsettes for.

For det andre innebærer den at prosessen med å bygge og opprettholde motstandskraft er en kontinuerlig prosess – man blir aldri ferdig.

Gjennomfør tiltak trinn for trinn.

Som Cyber Security Expert Simon Binder sier det: *«Jeg ser det som en sport. Du begynner ikke med de mest avanserte tingene først. Du begynner med å bygge opp en sterk kropp, et sterkt sinn, et sterkt grunnlag å stå på. Hvis du bygger et optimalt fundament, vil du kunne akselerere senere og konkurrere.»*



* I løpet av 2024 vil «administrer» tilføyes som den sjette komponenten i rammeverket. Mer informasjon finner du på *nist.gov/cyberframework*

«Vi har så mange brukere, noe som medfører en stor risiko for at noen vil åpne en e-post eller klikke på en lenke. Tidligere var det mer pinlig å innrømme at man hadde fått et virus. Det som er bra, er at man lærer av det. Hvilke erfaringer kan dere lære av for å styrke miljøet?»

IT- og sikkerhetssjef i offentlig sektor

Samarbeid og åpenhet skaper styrke

Partnerskap er veien å gå

Organisasjoner er utsatt for overhengende trusler. Forskningen vår er entydig: I fremtiden vil ingen organisasjon være i stand til å håndtere sikkerhet alene. Mangelen på dyktige sikkerhetsfagfolk, og de stadig mer integrerte økosystemene av partnere og forsyningskjeder som bedrifter opererer i, forårsaker sårbarhet. Partnerskap og samarbeid vil derfor være nøkkelen til å lykkes – enten det gjelder å styrke sikkerheten sammen med leverandører, *outsource* sikkerhetsarbeid eller dele læring og informasjon med andre aktører i bransjen.

Åpenhet bygger tillit

Vi vet alle at debatten går høyt om personvern. Beskyttelse av data er viktig for å bygge tillit. Effekten av den kommende EU-forordningen, kombinert med økende krav fra allmennheten og kunder, indikerer at større gjennomsiktighet og mer åpenhet vil være nødvendig i tiden som kommer. Ekspertene er samstemte om at åpenhet og ansvarlighet kan gjøre en forskjell, spesielt når man bygger tillit til kunder, media og andre sentrale interessenter.

Å finne den riktige sikkerhetsbalansen

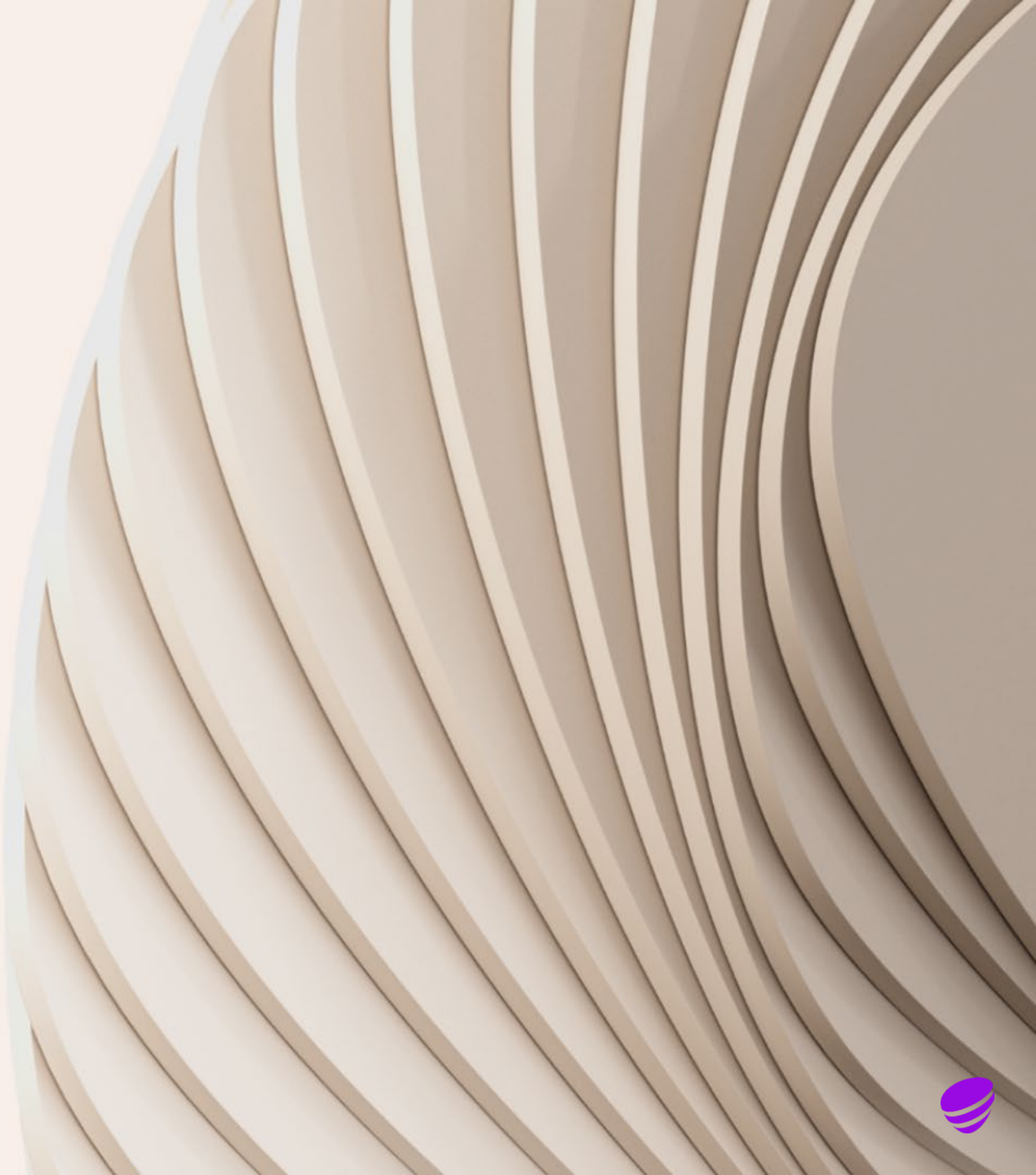
Det er nyttig å se på digital motstandskraft som en dynamisk balanse mellom mennesker, prosesser og teknologi. Det tar oss til den største utfordringen og muligheten i å bygge digital motstandskraft: menneskene.

94 %

av forbrukerne vil være mer lojale overfor merker som praktiserer åpenhet.
Kilde: Forbes

6

Det hackbare mennesket



Nr. 2

Lav sikkerhetsmodenhet blant medarbeidere rangeres som den nest største barrieren for å opprettholde tilstrekkelige sikkerhetsnivåer, etter begrensede budsjetter og ressurser.
Kilde: Radar, Cybersäkerhet 2024

«KI er for cybertrusler, det kjernefysikk er for krig.»

Håkan Kvarnström,
Head of Governance, Risk and Compliance i Telia

Den glemte elementet: Mennesker er det primære målet for fremtidige angrep

Det enkle, men nyttige PPT-rammeverket (People, Process, Technology) gjør det mulig for oss å undersøke hvordan de tre nøkkel-elementene i en hvilken som helst organisasjon virker sammen, og hvilke mønstre som viser seg på mikro- og makronivå som et resultat av dette.

Tidligere har investeringer i digital sikkerhet hovedsakelig blitt allokert til to av de tre områdene: teknologi og prosesser. Én åpenbar grunn til dette er at disse er håndgripelige: Ting og arbeidsmetoder er enkle, mens mennesker og bedriftskultur er komplisert.

Ledere har kanskje håpet på at «menneskebiten» ville falle naturlig på plass, så snart de andre elementene var i orden. Dessverre gjorde den ikke det.

Et overveldende flertall av angrep retter seg mot mennesker, og selv ikke den mest avanserte teknologi kan avverge at mennesker blir ofre. Enhver organisasjon som ønsker å få mest mulig ut av sine investeringer i digital sikkerhet, er nødt til å ta tak i dette kritiske faktumet. La oss derfor se nærmere på hva som gjør mennesker til hovedmålene for fremtidige angrep.

98 %

av cyberangrep benytter seg av sosial manipulering
Kilde: Splunk, State of Security 2024

52 %

av ledere mener med-arbeiderne mangler den nødvendige kunnskapen om cybersikkerhet
Kilde: Fortinet, Cybersecurity skills gap 2022

«Det er lettere å hacke et menneske enn en datamaskin.»

Anne-Marie Eklund Löwinder (Amel),
CEO og Cyber Security Expert

Tre faktorer setter mennesker i faresonen

01.
Hurtig innføring av KI er både en velsignelse og en forbannelse

Vi er for tiden vitne til et annet stort skifte innen bruk av teknologi, der organisasjoner utforsker KI-verktøy for å øke effektiviteten, eliminere kjedelige oppgaver og stimulere til kreativitet. Så langt er alt vel. Men det finnes en hake: Medarbeidernes ofte umodne bruk av KI-verktøy medfører en betydelig sikkerhetsrisiko og skaper en arena for cyberkriminelle.

Enkle handlinger som å kopiere og lime inn tekster i en offentlig KI-modell, kan avsløre sensitiv informasjon. Å mate disse modellene med konfidensielle data er en irreversibel prosess, og likevel er den gjennomsnittlige arbeidstakeren lite oppmerksom på risikoen. Mens noen foretak er ekstremt forsiktige, er det andre som mangler retningslinjer og overlater til medarbeiderne å navigere i KI-landskapet på egen hånd.

34 %

av bedriftene mangler en komplett strategi for generativ KI
Kilde: Splunk, Cybersecurity skills gap 2022

43 %

av sikkerhets-ansatte mener at KI kan hjelpe forsvarerne mer enn angriperne (opp fra 17 % på 8 måneder)
Kilde: Splunk, Cybersecurity skills gap 2022

02.
Angrep blir hyper-automatiserte (og det blir forsvaret, også!)

Phishing-e-poster står fortsatt for en stor andel av databruddene. Med KI kan hvem som helst angripe tusenvis av selskaper samtidig, og til og med skreddersy angrep for hver medarbeider. I takt med at *deepfakes* blir mer avanserte, har det nesten blitt umulig å skille mellom hva som er ekte og hva som er svindel.

Kriminelle utnytter følelsene våre ved å bruke «mørk psykologi» for å trigge autopilot-modusen vår, eller «System 1», slik nobelprisvinneren Daniel Kahneman har definert det. Dette systemet er refleksivt og emosjonelt, i motsetning til det mer bevisste «System 2», som krever tankearbeid. Vi forventer mye av medarbeiderne våre – fleksibilitet, evne til å bruke ny teknologi og balanse mellom arbeid og fritid – noe som gjør det nesten uunngåelig at noen tabber seg ut når de har hastverk eller er stresset.

USD 4,8 M

Gjennomsnitts-kostnad for organisasjoner rammet av brudd på grunn av phishing
Kilde: IBM, https://www.ibm.com/topics/phishing, 2024

03.
Livene våre blir infiltrert som aldri før

Hybridarbeid har visket ut skillelinjene mellom arbeid og fritid, noe som har medført nye digitale sikkerhetsrisikoer. Medarbeidere deler personlig og sensitiv informasjon daglig. Ledere oppfordres til å være åpne, noe som er gode nyheter for cyberkriminelle. Med tilgang til hobbyene, preferansene og aktivitetene våre blir «sosial manipulering» i den kunstige intelligensens tidsalder mer skremmende enn noensinne. *Deepfakes* er i ferd med å bli så overbevisende at de snart kan komme til å endre selve virkelighetsoppfatningen vår.

Så hva kan vi gjøre?

Intet menneske er en øy, og medarbeidere handler ikke i isolasjon. Organisasjoner har en enorm oppgave foran seg når de skal tilrettelegge for at sikkerhet kan ivaretas på en god måte. Derfor må vi nå rette oppmerksomheten mot kjernen i diskusjonen vår: kulturens rolle i å fremme digital motstandskraft.

46 %

Andel IT-fagfolk som rapporterer om en økning i angrep med sosial manipulering, direkte rettet mot enkeltpersoner
Kilde: LastPass, Combating Social Engineering in 2024

«Som organisasjon bør dere være veldig varsomme med å klandre de som har begått feil. Det er et lederansvar: Dere har ikke gitt medarbeiderne de rette betingelsene.

Åke Holmgren
Head of Cybersecurity and Secure Communications ved MSB, Myndigheten för samhällsskydd och beredskap i Sverige

CASESTUDIE

Laurynas Prikockis fra WSY Group Prioriter menneskene først

«Det er avgjørende at teamet som håndterer hendelsen, er forberedt fra et psykologisk perspektiv. Vi må forstå at medarbeidere er sårbare.»

Laurynas Prikockis er CIO i Western Shipyard Group. Tidligere i år ble selskapet utsatt for en betydelig cybersikkerhetshendelse der et phishing-angrep oppnådde tilgang til en medarbeiders brukernavn og passord, noe som medførte uautorisert tilgang til sensitiv informasjon.

Etterforskningen avdekket at phishing-e-posten utnyttet svakheter i selskapets implementering av flerfaktorautentisering, og at angrepet kunne ha vært avverget med bedre opplæring av og bevissthet hos medarbeiderne.

Laurynas, som også har en MBA-grad med blant annet psykologi, deler lærdommene sine fra hvordan han og teamet håndterte hendelsen ved å prioritere medarbeiderne.

Medarbeidersentrisk hendelsesrespons

Da bruddet skjedde, var sikkerhetsteamet i WSY i stand til å reagere raskt. De første tiltakene omfattet å tilbakestille passord og sikre berørte kontoer.

Viktigere var det at man la stor vekt på hensynet til den berørte medarbeideren, som umiddelbart ble kontaktet og informert om bruddet. WSY sørget også for psykologisk støtte for å bidra til å takle stresset i forbindelse med hendelsen.

Flerfaktorautentisering ble forsterket på alle plattformer. Sikkerhetsteamet gjennomførte en grundig granskning for å identifisere eventuelle ytterligere sårbarheter, og iverksatte tiltak for å ruste systemene sine mot lignende angrep.

Åpenhet i hele prosessen

Man holdt kommunikasjonen åpen for å sikre seg at medarbeideren forsto situasjonen og tiltakene som ble iverksatt for å redusere skaden.

Laurynas og sikkerhetsteamet jobbet tett med medarbeideren for å gjenopprette vedkommendes selvtillit, og sørge for nødvendig opplæring for å forebygge fremtidige hendelser.

Hendelsen ble rapportert til det nasjonale cybersikkerhetskontoret og andre relevante myndighetsinstanser for å overholde personvernregelverket. Selskapets responsplan omfattet også å varsle interessenter og allmennheten, og sikret dermed åpenhet om hendelsen og de iverksatte tiltakene.

Konklusjon

Hendelsen belyste viktigheten av en helhetlig tilnærming som balanserer tekniske tiltak med medarbeiderstøtte. Ved å fokusere på velferden til personen som var ansvarlig for bruddet, klarte selskapet ikke bare å begrense hendelsen på en effektiv måte, men også å fremme en kultur preget av tillit og digital motstandskraft. Ytterligere opplæringsøkter i cybersikkerhet ble gjennomført for alle ansatte, for å forbedre deres evne til å gjenkjenne og reagere på phishing-forsøk.

Saken viser oss at menneskesentrerte praksiser for cybersikkerhet er svært viktige i arbeidet med å takle og komme seg etter sikkerhetshendelser.

Dato for hendelse:
2. feb. 2024
Type angrep:
Phishing
Angrepsvektor:
En ondsinnet hacker lurte medarbeideren til å avsløre brukernavn og passord til sosiale kontoer og virksomhetens e-post.

Få med deg Laurynas' læringspunkter fra hendelsen!

WSY og Laurynas' sjekkliste
Læringspunkter fra hendelsen

Tre viktige poeng å ta med seg i arbeidet med å utforme en menneskesentrert tilnærming til sikkerhet.

01

Medarbeideres velferd

Det var svært viktig å prioritere den berørte medarbeiderens mentale helse og selvtillit. Det sikret at medarbeideren kunne fortsette som en verdsatt del av teamet, og bidro til å gjenoppbygge tillit internt i organisasjonen.

02

Styrket opplæring

Løpende utdannings- og opplæringsprogrammer ble etablert for å holde medarbeiderne oppdatert på de nyeste cybertruslene og beste praksiser.

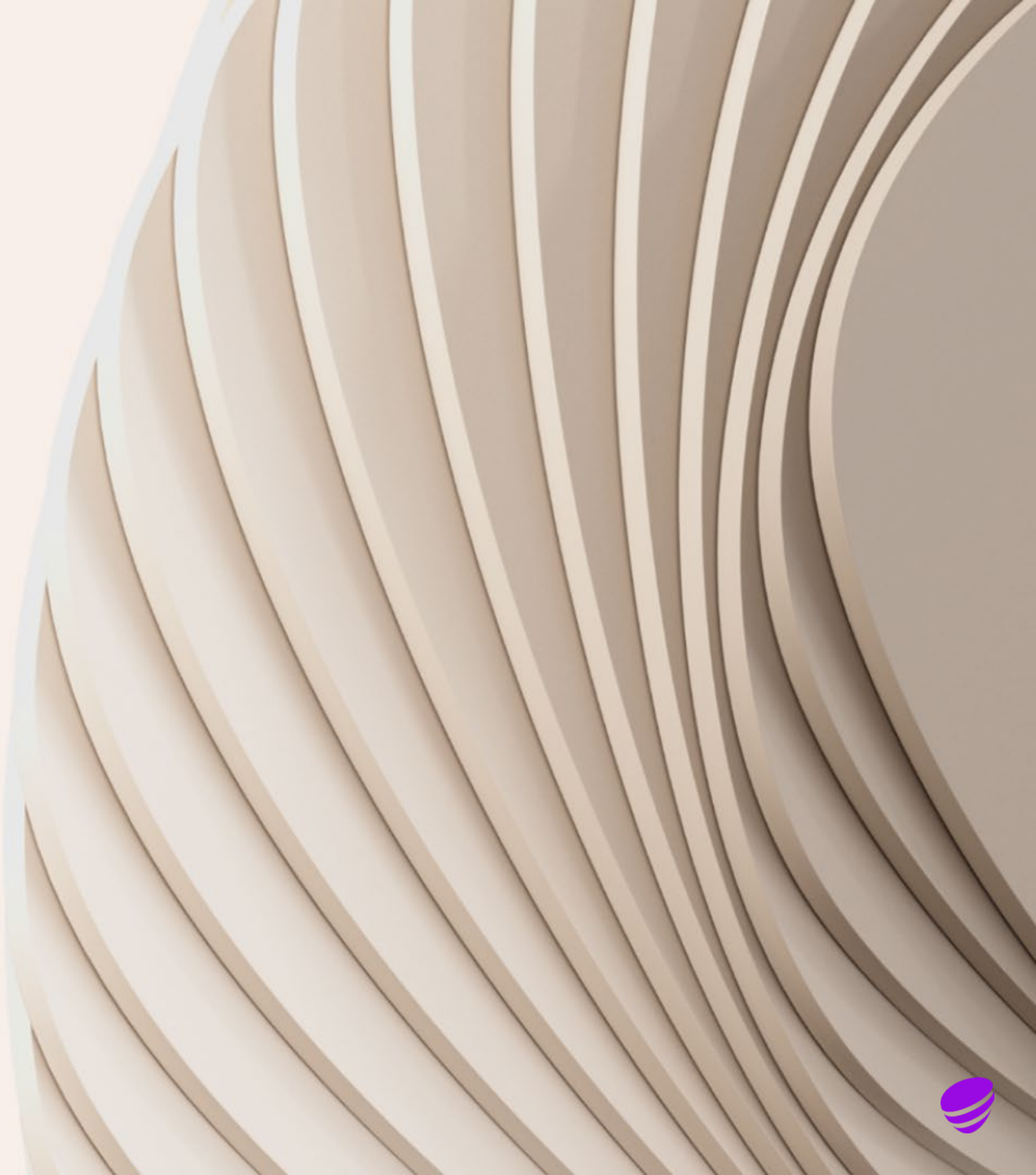
3

Forbedrede protokoller

Hendelsen utløste en gjennomgang og forbedring av eksisterende sikkerhets-protokoller, inkludert implementering av regelmessige sikkerhets-revisjoner og mer robuste løsninger for flerfaktor-autentisering.

07

Kultur som virkemiddel for sikkerhet



«Kultur er menneskers kollektive og samlede adferd. Vi trenger historiefortelling, opplæring, informasjon og diskusjoner.»

Håkan Kvarnström
Head of Governance, Risk and Compliance Telia

«Folkene våre og erfaringen deres er viktig – hvem som helst kan kjøpe ingredienser til en pasta carbonara, men ikke alle har ferdighetene til å lage en god en. Det samme kan sies om cybersikkerhet.»

Sam Rabar
Cyber Security Expert, Telia

Slik kan kultur være et sikkerhetsvirkemiddel

73 %

av medarbeidere sier at delaktighet i bedriftskulturen holder dem engasjert
Kilde: Seenit, The State of Employee Engagement, 2023

72 %

av ledere sier at kultur bidrar til vellykkede endringsinitiativer
Kilde: PWC, Global Culture Survey 2021

Phishing-e-poster, oppdatering av passord og det å slippe folk inn i kontorbygningen – alt dette er en del av arbeidshverdagen. Men hvordan bygger du en solid sikkerhetskultur?

Før vi går nærmere inn på det, la oss definere kultur som de felles verdiene, holdningene, overbevisningene og handlemåtene i en gruppe. Kort sagt, kultur lever i gruppemedlemmenes hjerter, sinn og hender.

Lederskap er viktig for endring

Å endre en etablert kultur er ingen enkel sak. Mange ledere forsøker naturligvis å endre hva medarbeiderne deres verdsetter og tror på. Det høres enkelt ut: definere den ønskede kulturen, kommunisere den og vente på at endringen skjer.

Vitenskapen viser oss imidlertid at denne tilnærmingen sjelden fungerer. Hvorfor ikke? Fordi verdier er dypt forankret og noe det tar tid å endre på. Selv om vi klarer å endre holdninger og overbevisninger, har vi fortsatt det notoriske gapet mellom kunnskap og handling. Tenk for eksempel på helse: Vi vet at det er sunt å trene, men unnlater ofte å gjøre det likevel. Bare å endre tankene fører sjelden til endringer i handlemåte.

Handling taler høyere enn ord

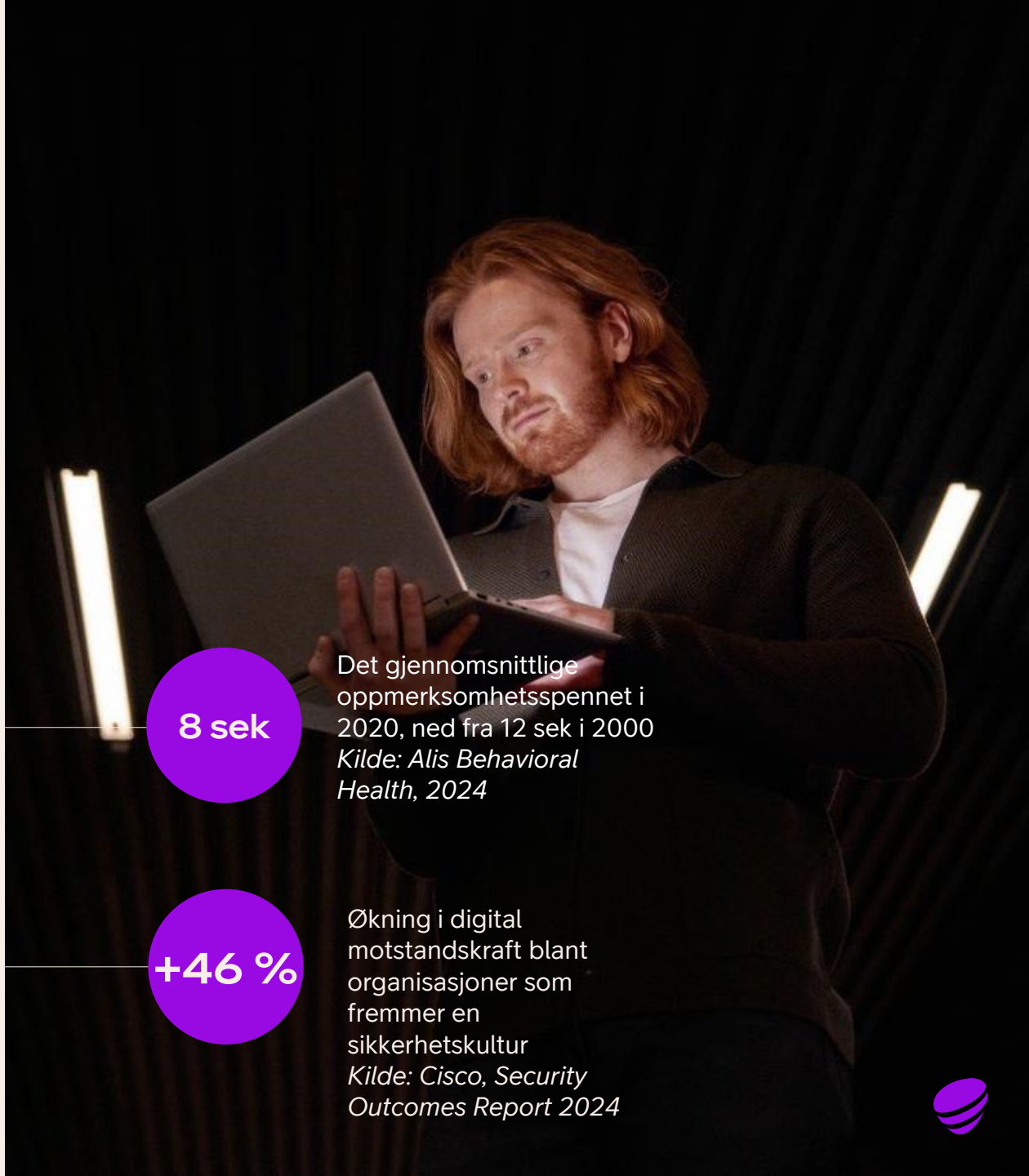
Her er de gode nyhetene: Å rette seg mot handlemønstre og beslutninger er den mest effektive måten å endre kultur på. Kjente akademiske studier indikerer tydelig at ledere bør fokusere på å få medarbeidere til å handle annerledes. Over tid vil nye adferds-mønstrene forme nye holdninger, over-bevisninger og verdier. En ny kultur vokser frem, drevet av praksis snarere enn prekener.

Gå foran med et godt eksempel

Lederskap er en avgjørende komponent i det å få medarbeidere til å opptre annerledes: Når ledere sier at sikkerhet er en topprioritet, men ikke selv oppfører seg i tråd med det, vil medarbeiderne selvsagt heller ikke gjøre det.

«En sikkerhetskultur kjennetegnes av bevissthet og hvordan den påvirker meg på daglig basis – enten vi snakker om å gå gjennom en dør eller åpne en e-post.»

IT- og sikkerhetssjef – teknologiselskap



8 sek

Det gjennomsnittlige oppmerksomhetsspennet i 2020, ned fra 12 sek i 2000
Kilde: Alis Behavioral Health, 2024

+46 %

Økning i digital motstandskraft blant organisasjoner som fremmer en sikkerhetskultur
Kilde: Cisco, Security Outcomes Report 2024

«For ti år siden diskuterte jeg ikke sikkerhet med ledelsen, det gikk mer på IT-service og stabilitet. 'Det er det opp til IT å håndtere, det er bare nødt til å virke.' Nå er det et emne på ledelsesnivå. Sikkerhet er en av virksomhetens grunnpilarer – vi snakker om sikkerhetskultur og sikkerhetsbevissthet.»

IT- og sikkerhetssjef, finanstjenesteselskap

CASESTUDIE

Thomas Zuliani fra Arla Foods
Viktigheten av sikkerhetskultur

«Du har teknologien, menneskene og prosessene. Men ingen av dem fungerer hvis du ikke har etablert en sikkerhetskultur i organisasjonen.»

Arla Foods er en stor leverandør av meieriprodukter med rundt 21 000 ansatte. I de 10 årene før Thomas Zuliani ble ansatt, hadde ikke Arla Foods hatt noen egen IT-sikkerhetssjef eller en ordentlig cybersikkerhetsavdeling. Dette hadde skapt et betydelig etterslep av sikkerhetsproblemer som trengte å håndteres.

Under Zulianis ledelse vokste cybersikkerhetsteamet hurtig fra to til tolv medlemmer for å takle disse utfordringene og etterleve det nye EU-regelverket.

Én stor utfordring var hvordan man skulle endre tenkemåten til en organisasjon som hadde unnlatt å prioritere cybersikkerhet i mange år. Å overvinne dette krevde vedvarende anstrengelser for å utdanne, skape engasjement og demonstrere verdien av proaktive sikkerhetstiltak.

Kulturens rolle innen cybersikkerhet

Zuliani understreker at suksessen til ethvert cybersikkerhetsprogram står og faller på kulturen i organisasjonen, og peker spesielt på tre nøkkelområder:

1. Toppledelsens engasjement:

Det er helt avgjørende at toppledelsen engasjerer seg. Zuliani påpeker at en administrerende direktør som prioriterer cybersikkerhet, kan drive organisasjonen mot høyere modenhetsnivåer innen sikkerhetspraksiser. Motsatt, hvis toppledelsen er likegyldig, blir det mye vanskeligere å nå det samme nivået av modenhet.

2. Proaktiv tenkemåte:

En proaktiv tilnærming til cybersikkerhet er helt vesentlig. Zuliani forklarer at mange organisasjoner bare responderer på cybersikkerhet etter at de har vært utsatt for en større uønsket hendelse. I Arla gjorde man imidlertid en bevisst innsats for å ta tak i sikkerheten proaktivt. Dette bidrar til å redusere risikoer før de utvikler seg til betydelige problemer.

3. Den menneskelige faktoren:

Mennesker er både det svakeste leddet og den største ressursen innen cybersikkerhet. Til tross for at det investeres millionbeløp i teknologi, utnytter de fleste vellykkede cyberangrep menneskelige sårbarheter, gjennom for eksempel phishing og sosial manipulering. Derfor er det avgjørende å forvandle medarbeidere til årvåkne forsvarere av organisasjonen.

Konklusjon

Zulianis lederskap illustrerer at en motstandsdyktig strategi for digital sikkerhet må omfatte mer enn bare teknologi og prosesser. Den krever en innarbeidet kultur av sikkerhetsbevissthet og proaktivt engasjement fra alle nivåer i organisasjonen, og spesielt toppledelsen. Ved å rendyrke en kultur der hver eneste medarbeider forstår sin egen rolle innen digital sikkerhet, kan organisasjoner forbedre sin digitale motstandskraft i betydelig grad.

Tilnærmingen reduserer ikke bare risiko, men forvandler også potensielle sårbarheter til styrker – og skaper en menneskelig brannmur som utfyller de teknologiske forsvarsmekanismene.

10

Nye medlemmer rekruttert til cybersikkerhets-teamet av Thomas i hans første år som CISO i Arla Foods, da teamet økte fra 2 til 12 personer

Få med deg Thomas' kultursjekkliste!

Arla Foods og Thomas' sjekkliste
Kultivering av sikkerhet

Fire grep som organisasjoner kan ta for å skape og hegne om en motstandsdyktig sikkerhetskultur

«Hvis en administrerende direktør ikke dyrker og sprer den kulturen vi ønsker å ha, blir det mye vanskeligere å oppnå cybermodenhet.»

01 Bevissthet og opplæring

Arla gjennomfører phishing-simuleringer og obligatorisk kursing for å holde medarbeiderne informerte og årvåkne vedrørende potensielle trusler. Kursøktene er utformet for å være engasjerende og relevante for medarbeidernes daglige arbeidsoppgaver.

02 Engasjerende aktiviteter

Zuliani er en sterk tilhenger av kreative strategier i innsatsen for å skape engasjement, som for eksempel en egen cybersikkerhetsmåned med aktiviteter, gjestetalere og åpne arrangementer. I tillegg til at disse aktivitetene utdanner alle ansatte, motiverer de dem også til å ta cybersikkerhet på alvor.

3 Gulrot fremfor pisk

I stedet for å kjøre en streng og dømmende stil foretrekker Zuliani en myk tilnærming, som oppmuntrer til samarbeid og felles ansvar. Dette inkluderer å delegere sikkerhetsansvar til medarbeidere og på den måten fremme en følelse av eierskap og årvåkenhet.

4 Integrert i strategien

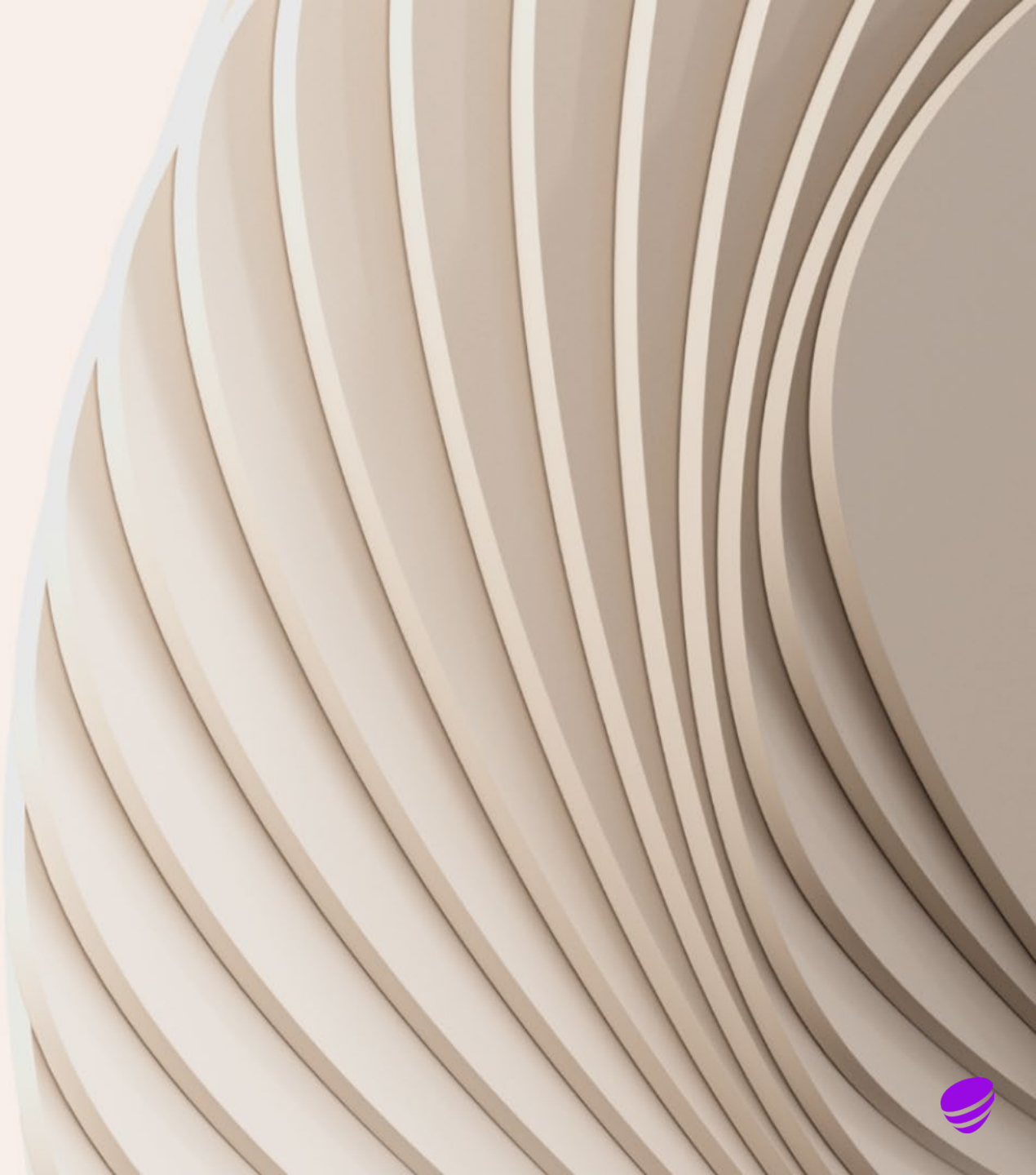
Mål for cybersikkerhet er integrert i selskapets overordnede misjon og visjon. For eksempel ved å sørge for at dataenes pålitelighet og integritet følger selskapets misjon om bærekraft og kvalitet i produksjonen av meieriprodukter.

«Etter hvert som vi blir mer datadrevne og bruker KI mer, blir vi også mer sårbare. Behovet for sikkerhet vil øke, og behovet for robusthet vil øke. Å bygge digital motstandskraft er avgjørende. Det gjelder ikke bare for hvordan vi designer ting på en sikker måte, men også hvordan vi får medarbeidere til å føle seg trygge i utførelsen av jobbene sine.»

Magnus Leonhardt
Security & Strategy Expert, Telia

08

Slik bygger man en sikkerhets-kultur: de fem hovedpunktene



«Innstillingen vi har til datasikkerhet er grunnlaget for digital motstandskraft. Det setter enkeltpersoner i stand til å gjenkjenne risiko og handle proaktivt for å beskytte, ikke bare seg selv, men hele organisasjonen og samfunnet.»

Malin Fransén Kronberg
Head of Security, Telia

Oppskriften på digital motstandskraft: Sikkerhetskulturens fem byggesteiner

Vi har identifisert fem mønstre som gjerne går igjen i modne sikkerhetsorganisasjoner. Disse kjennetegnene bidrar alle til å utvikle en motstandsdyktig sikkerhetskultur, ved at de setter enkeltpersoner i stand til å delta aktivt, lære og utvikle seg.

01
Ps
Psykologisk sikkerhet

02
Mp
Mild paranoia

03
Nf
Null friksjon

04
Fp
Forskjellige perspektiver

05
Kl
Kontinuerlig læring

«Sikkerhetskultur innebærer å kunne snakke om det. Ingen bør bebreides for å innrømme noe.»

Michael Mothander
Cyber Security Expert, Telia

01. Psykologisk sikkerhet

Tradisjonelt har mange organisasjoner opplevd en kultur der digital sikkerhet er omgitt av taushet og skam. Medarbeidere har vært redde for å begå og innrømme at de har begått feil, og organisasjoner har forholdt seg tause i kjølvannet av angrep.

Bedrifter med digital motstandskraft følger retningslinjer der bebreidelser og skam ikke er en del av pakken. Medarbeiderne er ikke redde for å begå feil, og føler at det er trygt å rapportere dem dersom de skulle forekomme. De risikerer ingen trusler eller sanksjoner hvis de har trådt feil. Eksperter med spesialkompetanse er de første som responderer og tilbyr støtte til sårbare medarbeidere som har blitt lurt og utnyttet av svindelaktører.

Åpenhet er en nøkkelkomponent i psykologisk sikkerhet: Ekspertene kommuniserer ærlig med medarbeidere og interessenter når hendelser inntreffer. Dette bidrar i sin tur til å bygge gjensidig tillit, og medarbeiderne føler at de trygt kan fortelle om det som har skjedd.

Måling av psykologisk sikkerhet blant medarbeidere

*Spørreskjema utarbeidet av Harvard-professor Amy Edmondson**

1	2	3	4	5	6	7
Hvis du begår en feil i dette teamet, blir det ikke brukt mot deg.	Team-medlemmene kan ta opp problemer og vanskelige emner.	Team-medlemmene aksepterer at andre ikke er som dem selv.	Det er trygt å ta en risiko i dette teamet.	Det er ikke vanskelig å be andre team-medlemmer om hjelp.	Ingen vil forsettlig gjøre noe for å undergrave arbeidet mitt.	De unike ferdighetene mine blir verdsatt og utnyttet.

** Test medarbeiderne dine på fearlessorganizationscan.com*

02. Mild paranoia

Folk flest har vært altfor tillitsfulle i forbindelse med cyberangrep, kanskje på grunn av angrepenes abstrakte og ofte indirekte natur. Manglende årvåkenheten har vært en gavepakke til trusselaktørene.

Motstandsdyktige organisasjoner har klart å konkretisere og belyse risikoene, og på den måten mobilisert til årvåkenhet i hele selskapet. De har gjort dette uten å ta det for langt i retning av panikk eller resignasjon. Som Niclas Jalvinger, CISO/CSO i Telia, har uttalt, er nøkkelordet her *mild paranoia*, en økt risikobevissthet kombinert med sunt bondevett.

I forbindelse med psykologisk sikkerhet: Overrapportering er alltid bedre enn underrapportering. Den eneste trusselen som kan unngås, er den trusselen som har blitt oppdaget.

Niclas Jalvingers topp 3

Telias CISO/CSO deler sine tips om hvordan man bygger en bedriftskultur preget av sikkerhet i alle ledd

1

La handling følge ord
Ledere kan ikke stå på barrikadene og snakke om sikkerhet uten selv å gå foran som et godt eksempel. Det starter på toppen.

2

Lytt mer, snakk mindre
Gå aldri ut fra at du vet mer enn medarbeiderne. Det er mye å lære bare ved å lytte i stedet for å snakke.

3

Tenk som en kriminell
Oppmuntre medarbeiderne til å forestille seg måter kriminelle kan angripe selskapet på, for å styrke bevisstheten.

“Bedriftens sikkerhetspolicy må være beskrevet så alle forstår det, ikke bare sikkerhetsekspertene.”

Sam Rabar
Cyber Security Expert, Telia

03. Null friksjon

Som vi har sett, risikerer organisasjoner som er avhengige av at medarbeiderne i utgangspunktet må være svært bevisste, klartenkte og kunnskapsrike for å kunne gjøre jobbene sine, å mislykkes.

Organisasjoner med digital motstandskraft forsøker ikke å overvinne menneskets natur, men tilpasser i stedet sikkerhetsarbeidet sitt deretter. De innarbeider i størst mulig grad sikkerhets-teknologi og -prosesser i eksisterende adferdsmønstre og arbeidsflyter, heller enn å påtvinge medarbeiderne nye måter å jobbe på. Nøkkelen er å appellere til det som betyr noe for folk: å få individuelle og jobbrelaterte incentiver til å dra i samme retning.

De mange akronymene og forkortelsene som brukes innen digital sikkerhet, gjør emnet både uklart og ekskluderende.

Motstandsdyktige organisasjoner reduserer friksjon, simpelthen ved å bruke et enkelt og tydelig sikkerhetsspråk for å minimalisere den mentale anstrengelsen og unngå risikoen for misforståelser. Og ikke minst forstår de at det ikke finnes noen universalløsning for sikkerhet: Budskap må skreddersys for ulike mottakere, slik at folk husker dem og blir engasjert.

Et annet friksjonspunkt er utydelige kommunikasjonskanaler: ikke å vite hva man skal gjøre eller hvem man skal henvende seg til når trusler dukker opp. Organisasjoner med digital motstandskraft har tydelige rutiner for å forenkle og oppmuntre til rapportering.

3 tips for minske friksjon

Organisasjoner med digital motstandskraft jobber med – ikke mot – menneskets natur.

1

Søk eksperthjelp
Allier deg med eksperter på menneskelig adferd og psykologi for å oppnå varige endringer.

2

Bruk et enklere språk
Samarbeid med kommunikasjons-avdelingen og finn et felles språk for digital sikkerhet – som alle forstår.

3

Appeller til folks egeninteresse
Mennesker støtter det de kan skape. Du får lettere gjennomslag hvis du fokuserer på det som motiverer folk i det daglige arbeidet deres.

04. Forskjellige perspektiver

Digital sikkerhet har tradisjonelt vært et mannsdominert, homogent felt: Mange fagfolk har lignende bakgrunner, erfaringer, kunnskaper og kulturelle referanser. Dette åpner for den svært reelle risikoen for uoppmerksom blindhet, som inntreffer når personer ikke klarer å få øye på uventede stimuli som er klart synlige.

I et berømt eksperiment undersøkte 24 radiologer en serie røntgenbilder av lunger for å lete etter klumper. En gorilla, 48 ganger større enn en gjennomsnittlig klump, var satt inn i det siste røntgenbildet. 83 prosent av radiologene så ikke gorillaen.

Organisasjoner med digital motstandskraft involverer medarbeiderne i sikkerhetsarbeidet og drar fordel av det faktum at et mangfold av perspektiver øker sjansen for å oppdage og unngå en trussel. De ser utenfor tradisjonelle møteplasser og inviterer nye ferdigheter til bordet: Adferdsforskere, hackere og eks-militære kan alle bidra til å forme fremtidens sikkerhetsekspertise.

3 tips som utvider perspektivet

Enkle knep for å evne å se situasjonen med et nytt blikk.

1

Erkjenn dine egne fordommer

Team med lignende bakgrunner og perspektiver risikerer å overse kritiske sikkerhetsfaktorer. Identifiser mulige fordommer og bring inn nye perspektiver.

2

Søk allsidig kompetanse

Kriminelle handler raskt. Utfordre tradisjonene ved å hente inn ny kompetanse – adferdseksperter, analytikere og prosessledere har topprangerte ferdigheter, som kan ruste teamet ditt for fremtiden.

3

Finn nye venner

Skap strukturerte samarbeid rundt digital sikkerhet ved å trekke inn viktige interessenter og avdelinger internt – fra HR, kommunikasjon og juridisk til toppledelsen.

«Mennesker og organisasjoner elsker å lære av sine egne feil – andres feil kan gi opphav til gode historier, men de beveger deg aldri på samme måte som dine egne.»

Mehis Hakkaja,
Grunnlegger, CEO og eier av
Clarified Security OÜ

05. Kontinuerlig læring

Mange organisasjoner erkjenner ikke viktigheten av å gi medarbeidere tid og ressurser til kompetanseheving, noe som gjør dem skjøre når de stilles overfor hurtige forandringer.

Organisasjoner med digital motstandskraft utstyrer medarbeiderne sine med kunnskap og verktøy, men oppmuntrer også til nysgjerrighet og kontinuerlig læring. I tråd med ønsket om å oppnå null friksjon er de nøye med å utarbeide og gjennomføre utdanningstilbudene sine på en måte som gjør dem tiltrekkende, minneverdige og enkle å omsette i handling.

De benytter teknikker fra adferdsforskningen, som for eksempel mikrovaner, for å minimalisere energikostnader og maksimalisere effekter. Medarbeiderne belemres ikke med mer informasjon eller instruksjon enn det som er nødvendig for å opptre sikkert i den spesifikke rollen de har i organisasjonen.

Når uønskede hendelser inntreffer, ser de dem som muligheter til å lære og vokse. Kontinuerlig læring gjennom handling – praktisk erfaring – er i høy grad betegnende for digital motstandskraft, og er en konkret metode for å bygge opp kunnskapskapitalen i organisasjonen.

Til slutt bør det nevnes at selv om bedriftene våre konkurrerer om kunder og kontrakter, bør vi alle samarbeide om sikkerhet. Å dele erfaringer på tvers av bransjer, beskytter bedriftenes datasystemer og bidrar til et tryggere organisasjonsmiljø for alle.

3 kompetanseløft

Fang medarbeidernes oppmerksomhet og skap engasjement.

1

Rapporteringsrutiner
Sørg for at medarbeidere har riktige verktøy og prosesser for å lære og rapportere – enkle å forstå og bruke.

2

Lær sammen med andre
Se virkelige hendelser som muligheter til å diskutere, samarbeide, dele læring og tilpasse dere. Vurder å søke samarbeid med eksterne partnere.

3

Gjør læring engasjerende
Bruk virkelige saker og eksempler for å inspirere (og advare). Eksperimenter med nye formater, som spillifisering, podkaster eller gjestetalere.

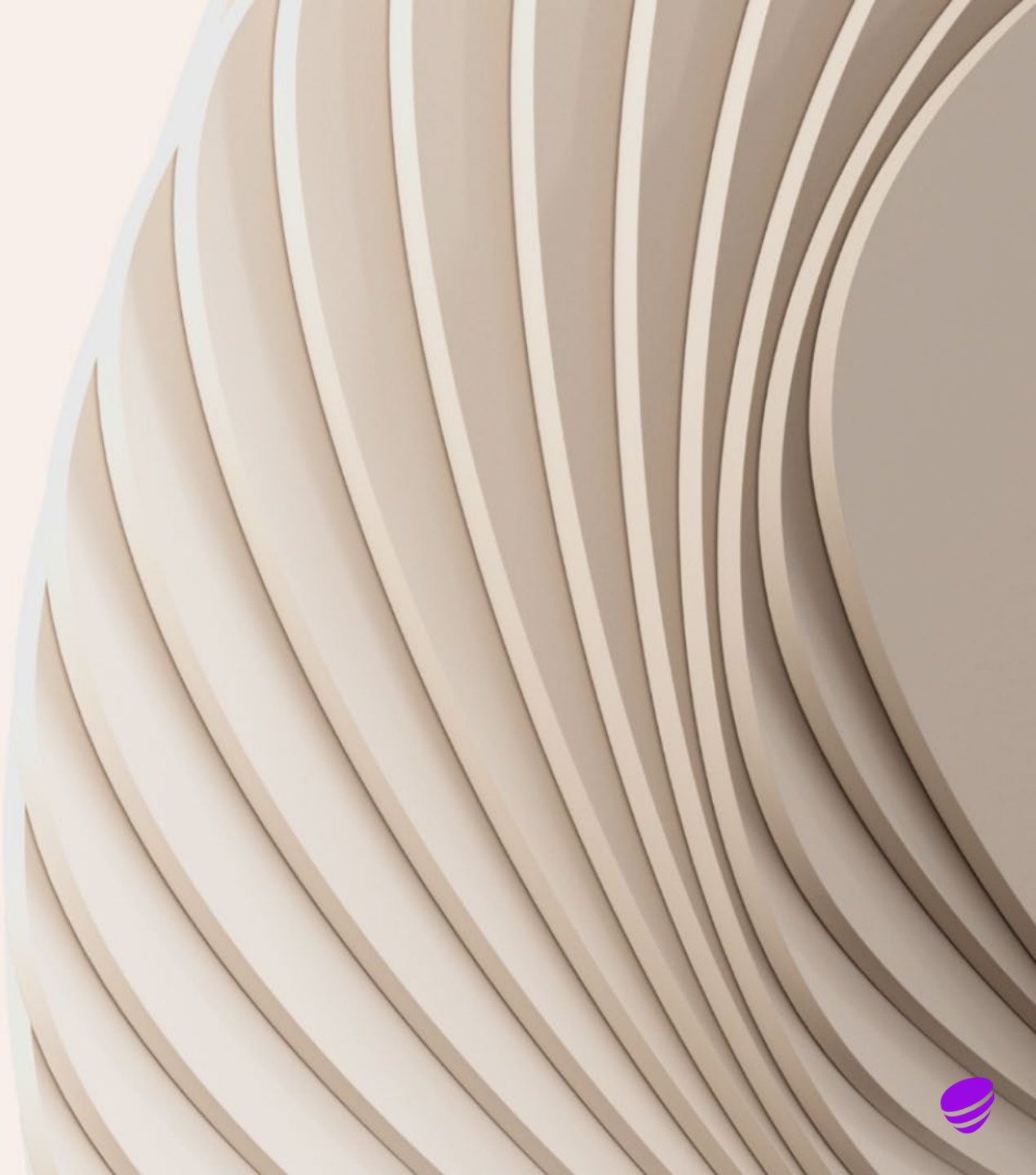
Oppskriften på digital motstandskraft: Fem tiltak å gjennomføre

Det tar tid å endre vaner – selv når det ikke er vår egen overlevelse som står på spill. Det er tydelig at det ikke er nok å anskaffe de riktige sikkerhetsverktøyene og -prosessene. Du er også nødt til å få medarbeiderne til å begynne å bruke dem. Dette er fem tiltak som må gjennomføres for å bygge en motstandsdyktig sikkerhetskultur.

01	02	03	04	05
Ps	**Mp**	**Nf**	**Fp**	**Kl**
Psykologisk sikkerhet	Mild paranoia	Null friksjon	Forskjellige perspektiver	Kontinuerlig læring
Gjør det til et trygt rom	Gjør det til en prioritet for ledelsen	Gjør det enkelt	Gjør det inkluderende	Gjør det engasjerende

09

Konklusjon



Sammen står vi sterkere

Digital motstandskraft er vår aller viktigste ressurs for å kunne manøvrere i en digital tidsalder der endringshastigheten bare øker. Slik sikkerhetsbeltet revolusjonerte bilsikkerheten, kan en aktiv digital sikkerhetskultur beskytte organisasjonene våre mot et trusselbilde i stadig utvikling. Ved aktivt å vurdere risikoer og dyrke en kultur med kontinuerlig læring og tilpasningsdyktighet, kan vi omgjøre sårbarhet til styrke.

Fremtiden tilhører dem som er forberedt på den. La oss ta disse prinsippene i bruk for å bygge et sikkert fundament basert på partnerskap og åpenhet. Først da kan vi bevege oss trygt mot en sikrere og smartere morgendag.

Ingen kan løse dette på egen hånd, så la oss slå kreftene sammen! Sammen kan vi snu utfordringer til muligheter – og sørge for at de digitale motorveiene er like sikre som de er raske.

Hvis du ønsker å fortsette denne diskusjonen eller lære mer, så ta kontakt med oss i Telia.

Vedlegg

Bidragsytere til rapporten

Bidragsytere fra Telia	Rolle	Organisasjon
Aurimas Žlibinas	Head of Enterprise	Telia Litauen
Kristjan Kukk	Head of B2B	Telia Estland
Conor McGlynn	Head of Security Strategy and Transformation	Telia Company
Håkan Kvarnström	Head of Governance, Risk and Compliance	Telia Company
Ida La Spisa	CIO	Telia Sverige
Jon Christian Hillestad	Head of Enterprise	Telia Norge
Kristofer Ågren	Head of Product, Division X	Telia Company
Magnus Leonhardt	Head of Strategy & Innovation	Telia Sverige
Malin Fransén Kronberg	Head of Security	Telia Sverige
Mats Mägiste	Security Infrastructure Expert	Telia Sverige
Michael Mothander	Cyber Security Expert	Telia Cygate
Minna Vyyrylainen	Head of Business Networking	Telia Company
Nicholas Rundbom	Head of Communications B2B	Telia Sverige
Nicklas Olofsson	Culture and growth	Telia Company
Niclas Jalvinger	Group CISO / CSO	Telia Company
Ola Rembe	Head of Brand, Communications & Sustainability	Telia Company
Olli Pirttijärvi	Head of B2B	Telia Finland
Patrik Holmqvist	COO	Telia Cygate
Pontus Eklöf	Senior Sales Specialist	Telia Company
Sam Rabar	Cyber Security Expert	Telia Company
Sigrid Reijnst	Head of Employer Brand	Telia Company
Simon Binder	Cyber Security Expert	Telia Cygate
Thomas Johansson	Global Business Strategy	Telia Company
Tobias Larsson	Head of B2B Sweden	Telia Sverige
Tomas Eklind	Portfolio Manager	Telia Company
Vinicius Joaquim Camargo	Division X	Telia Company
Zackaria Bennani	Portfolio Manager	Telia Cygate

Rapportens prosjektteam	Rolle	Organisering
Emelie Aidehag	Head of Insight & Foresight	Telia Company
Magnus Fahlgren	Brand Insight Manager	Telia Company
Suzanne Tellström	Brand Management	Telia Company

Eksterne eksperter	Rolle
Anne-Marie Eklund Löwinder	CEO og grunnlegger Amelsec, kjent cybersikkerhetsekspert og tidligere kryptoansvarlig
Mehis Hakkaja	Grunnlegger, CEO og eier av Clarified Security OÜ
Pontus Johnson	Professor KTH og direktør i Center Cyber Defense and Information Security
Åke Holmgren	Head of Cybersecurity and Secure Communications i MSB, Myndigheten för samhällsskydd och beredskap i Sverige

Forskningsbyråteam	Rolle
Alexis Bolonassos	Research Strategist i Augur
Jenny Franzén Lycke	Foresight Director i Augur

Referanser

Albarracin, D. et al. (2024). Determinants of behavior and their efficacy as targets of behavioral change interventions

Alis Behavioral Health (2024) https://www.alisbh.com/blog/ average-human-attention-span-statistics-and-facts

Allianz Commercial. (2023). *Cyber security trends 2023.*

Barreto, H. (2024). *The secret to creating brand loyalty. Forbes*

Brooks, C. (2023). *Cybersecurity Trends & Statistics for 2023; What You Need To Know.* Forbes.

Cisco. (2024). *Security Outcomes Report Vol. 3. Achieving Security Resilience.*

Click. (2024). *A no bullshit paper: A manifesto for Effortless Culture Change.*

Deloitte: (2022). *Global Future of Cyber Survey 2023. Building long-term value by putting cyber at the heart of the business.*

Europaparlamentets forskningstjeneste. (2023). *The NIS2 Directive. A high common level of cybersecurity in the EU*

Farnam Street (2021) *The Great Mental Models Volume 2: Physics, Chemistry, and Biology*

Fortanix. (2023). *Preparing for post-quantum cryptography. Mapping your organization's data security strategy to the effects of quantum computing*

Fortinet (2022). *Cybersecurity skills gap.*

Gartner. (2023). *Gartner Identifies the Top Cybersecurity Trends for 2023.* [pressemelding]

Heino, M et al. (2024) *From a false sense of safety to resilience under uncertainty.*

IBM (2024) https://www.ibm.com/topics/phishing

LastPass (2024). *Combating Social Engineering in 2024.*

International Telecommunication Union. (2021).

McKinsey & Company. (2022). *Cybersecurity trends: Looking over the horizon.*

Pentera (2024) *The State of Pentesting 2024*

PWC (2021), *Global Culture Survey.*

Radar. (2024). *Cybersäkerhet 2024. Från verksamhet till ekosystem.*

Seenit (2023). *The State of Employee Engagement.*

Sentor. (2021). *ISO 27001. En introduktion till standarden.*

Snowflake. (2024). *Data + AI predictions 2024.*

Splunk (2024). *State of Security 2024: The Race to Harness AI*

SVT (2024), *Allvarliga brister i svenska myndigheters cybersäkerhet*

Telenor. (2024). *Digital Security 2023. It gets serious.*

Telia (2024) *Telia Digital Index (2024).*

Verdens økonomiske forum. (2024). *The Global Risks Report 2024.*

Verdens økonomiske forum. (2024). *Global Cybersecurity Oulook 2024.*