ZERO TRUST

SOLDIER

ENISA Threat Landscape 2022

This is the tenth edition of the ENISA Threat Landscape (ETL) report, an annual report on the status of the cybersecurity threat landscape. It identifies the top threats, major trends observed with respect to threats, threat actors and attack techniques, as well as impact and motivation analysis. It also describes relevant mitigation measures. This year's work has again been supported by ENISA's ad hoc Working Group on Cybersecurity Threat Landscapes (CTL).

Published November 03, 2022
Language

The ENISA Threat Landscape (ETL) report is the annual report of the European Union Agency for Cybersecurity, ENISA, on the state of the cybersecurity threat landscape. In October 2022, ENISA released the 10th edition of the report that covers a period of reporting starting from April 2021 up to July 2022:

1. **Ransomware**
2. **Malware**
3. **Social engineering**
4. **Threats against data**
5. **Threats against availability: Denial of Service**
6. **Threats against availability: Internet threats**
7. **Disinformation – misinformation**
8. **Supply-chain attacks**

ENISA THREAT LANDSCAPE 2022

enisa

EUROPEAN UNION AGENCY FOR CYBERSECURITY

GÖRAN TÖMTE

Hvem er ansvarlig?
Systemet eller menneskene?

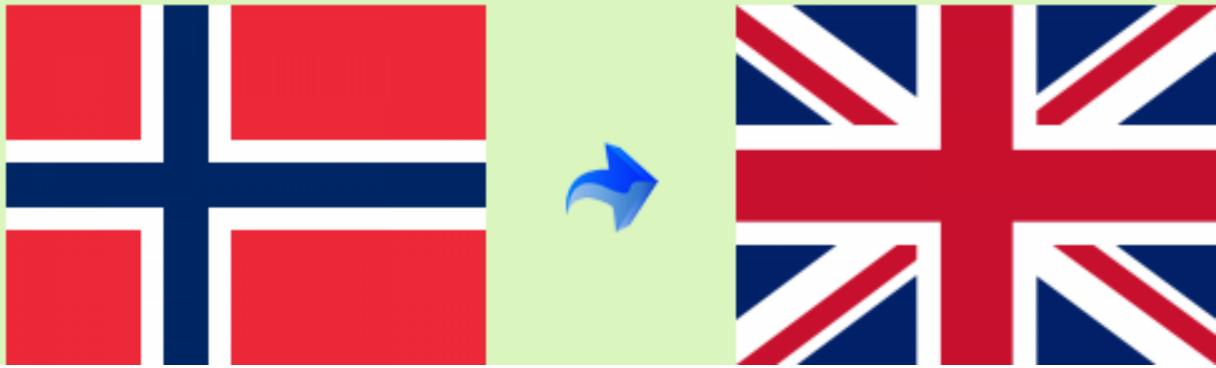
ZERO TRUST
SOLDIER

System vs mennesker

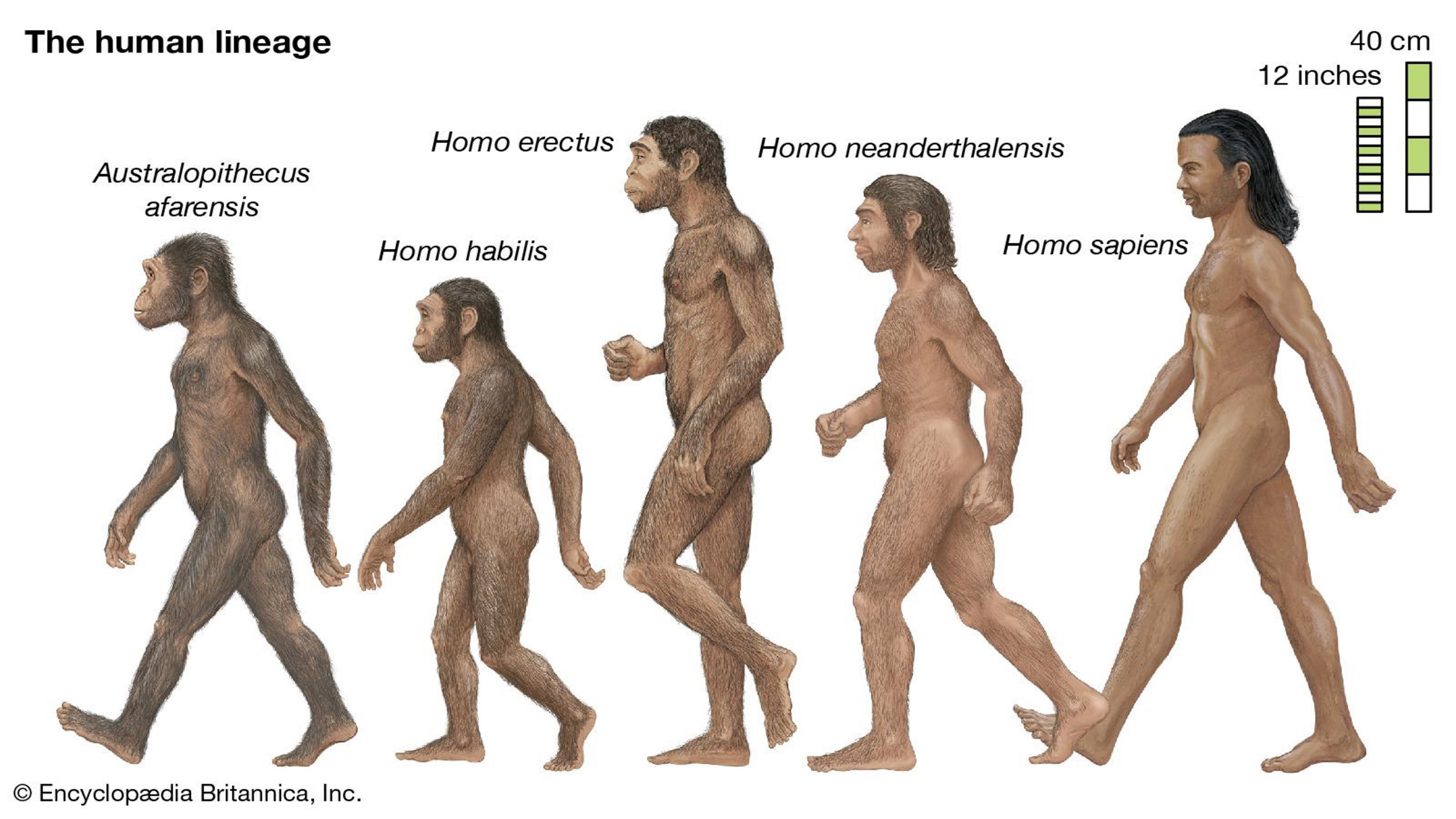
ZERO TRUST
SOLDIER

Norwegian-English translation in context

Systemsvikt in English

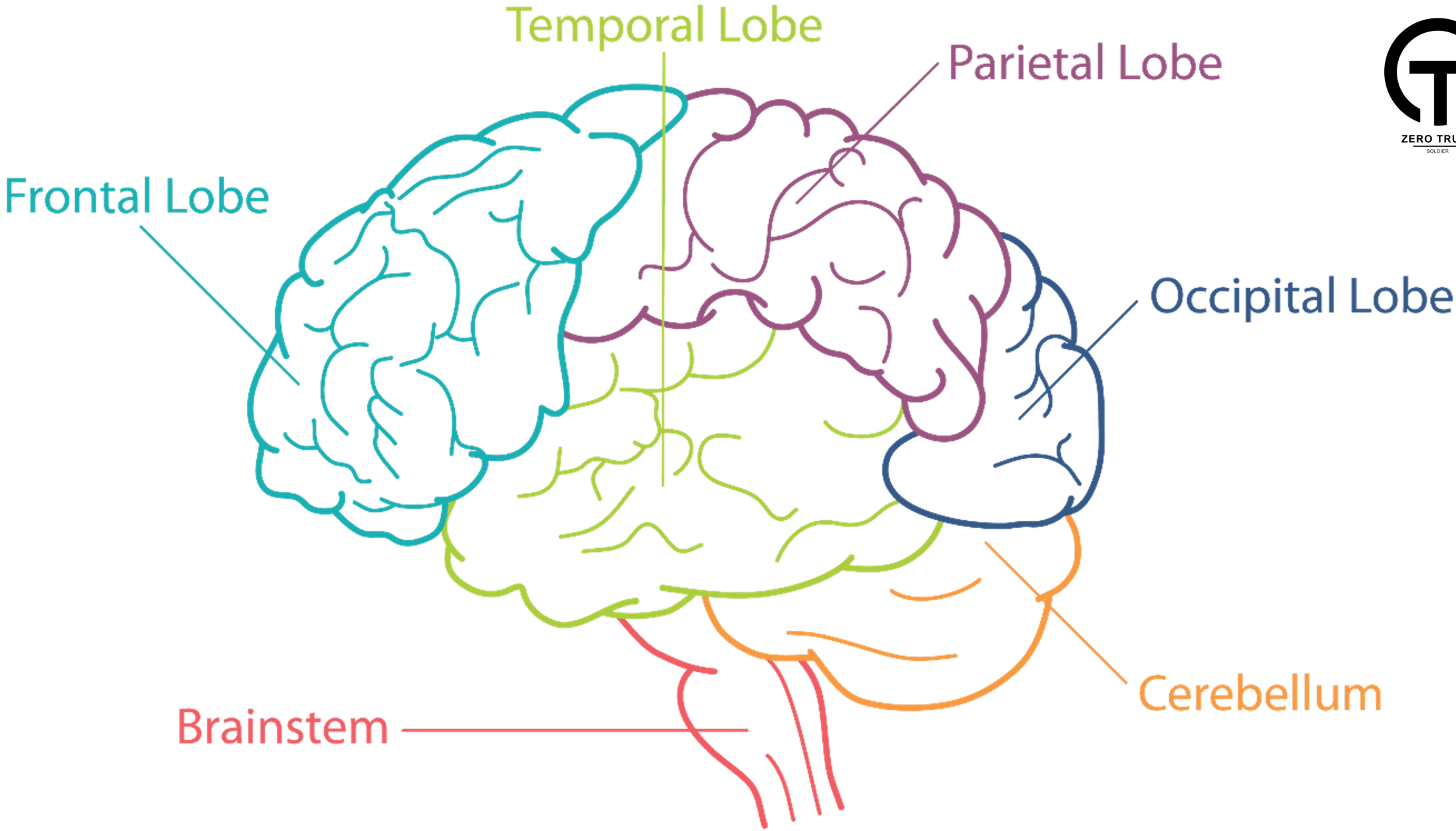


TR-EX.ME




NSM Podkast 188 - Mennesker mennesker og atter mennesker
Nasjonal sikkerhetsmyndighet (NSM)
3 days ago
Technology
4:07
19:07
NSM
En podkast om sikkerhet, mennesker, teknologi og samfunn.

ZERO TRUST
SOLDIER



ZERO TRUST
SOLDIER

ZERO TRUST
SOLDIER

ZERO TRUST
SOLDIER

Kompetanse

ZERO TRUST
SOLDIER

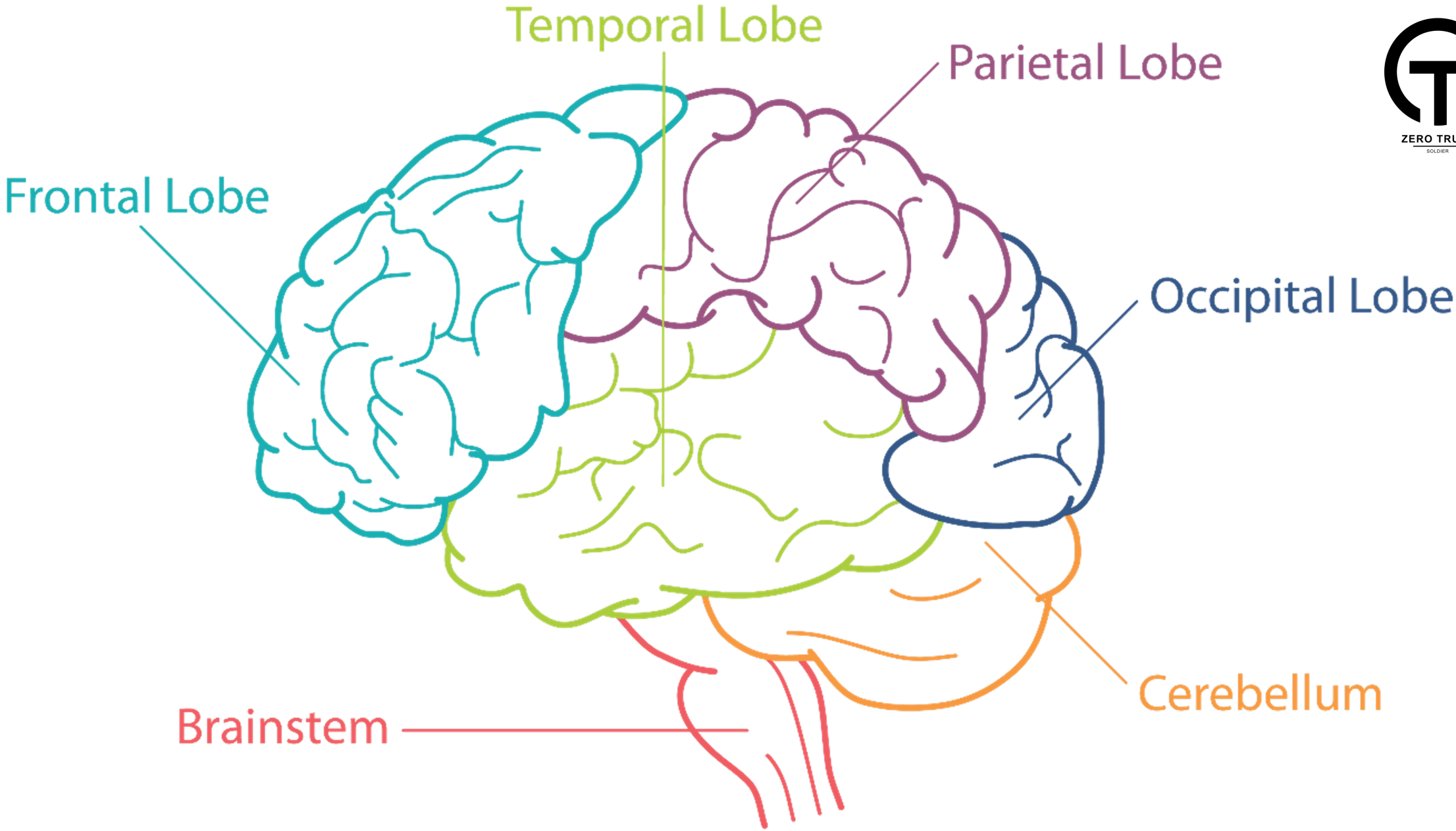
Bevissthet

ZERO TRUST
SOLDIER

Ydmykhet

ZERO TRUST
SOLDIER

Lidenskap



ZERO TRUST
SOLDIER

ZERO TRUST
SOLDIER

En historie fra virkeligheten

ZERO TRUST
SOLDIER

ZERO TRUST
SOLDIER

IT fikser det
Vi har tjenesteutsatt

GÖRAN TÖMTE

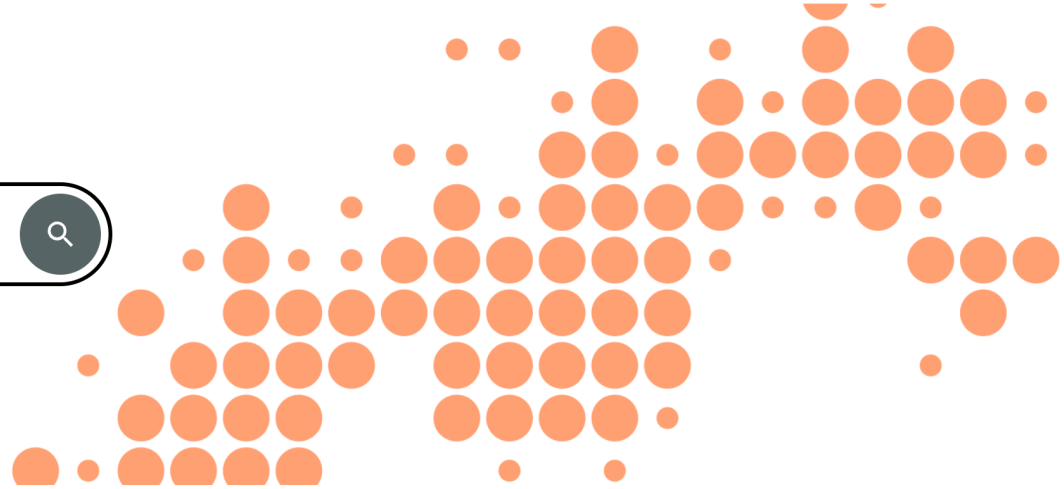
Det skjer ikke oss, så hvorfor bry seg? Dessuten fikser IT det... I tillegg har vi tjenesteutsatt flere ting

Hva kan vi hjelpe deg med?

Søk her

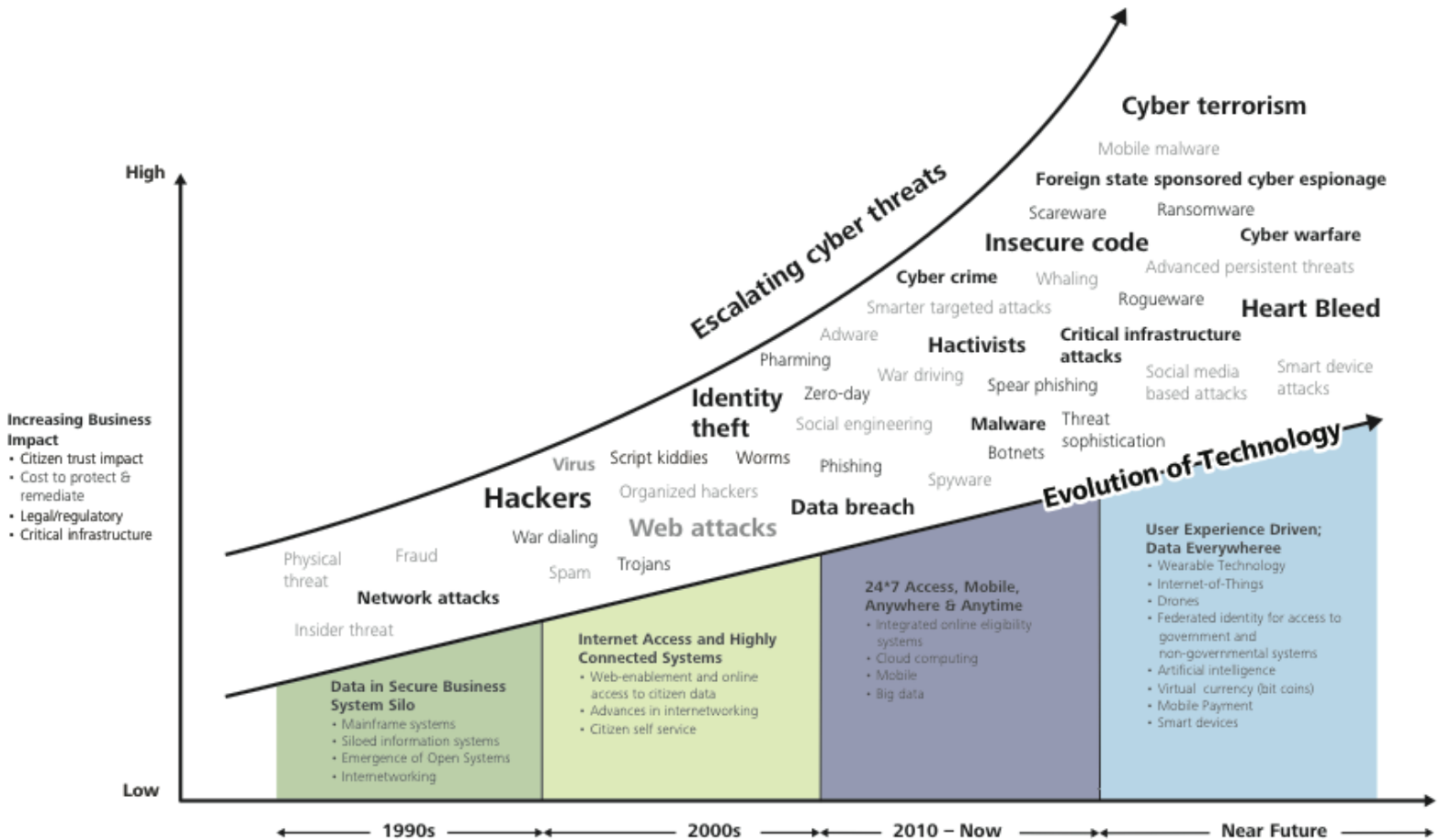
Søk

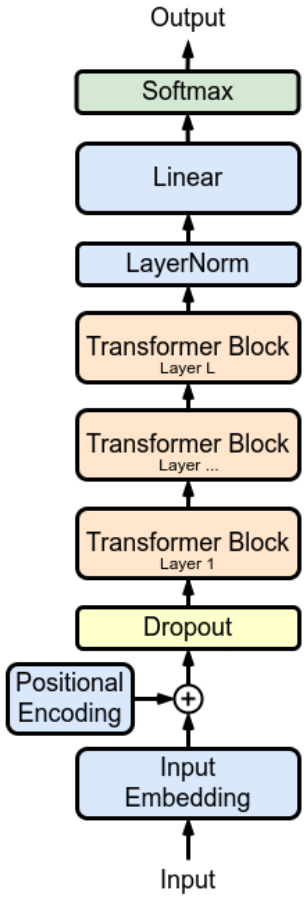
Fylkestingsvalget 2023 Politikk Finn ansatt Tiltakssonen

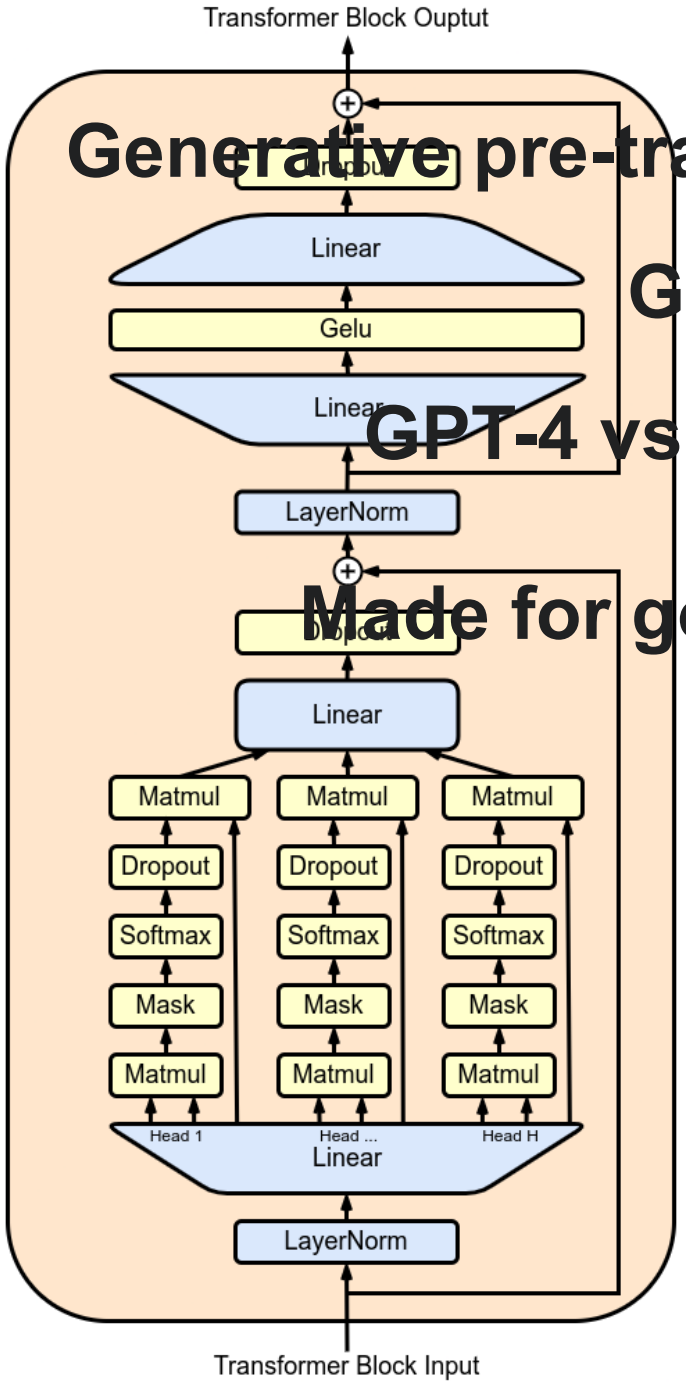


- → Skole og opplæring
- → Tannhelse
- → Kultur
- → Natur, klima og miljø
- → Samisk og kvensk/norskfinsk
- → Plan og høringer
- → Samferdsel
- → Næringsutvikling
- → Kulturarv
- → Folkehelse, idrett og friluftsliv
- → Internasjonalt
- → Støtte, stipend og priser


'scan input pin
if Button(GPIO, 5, 10, 1) then
state = true
else
state = false
end if
if state <> oldstate then
if state = true then
' change true/false below depending on whether
' device goes high or low on triggering.
transmit2(false)
oldstate = state
end if
if state = false then
' send the opposite of above (change
transmit2(true)
oldstate = state
end if
end if
end sub
main:
assign prescaler to TMR0
lngCounter = lngCounter + 1
if lngCounter = 11377 Then
lngCounter = 0
end if
minutes = minutes +1
end if
if minutes = 10 then
transmit(binAlermSignal)
end if
end if
minutes = 0
end if


High
Low
Increasing Business Impact
• Citizen trust impact
• Cost to protect & remediate
• Legal/regulatory
• Critical infrastructure
Escalating cyber threats
Evolution of Technology
Cyber terrorism
Mobile malware
Foreign state sponsored cyber espionage
Scareware
Ransomware
Insecure code
Cyber warfare
Advanced persistent threats
Cyber crime
Whaling
Rogueware
Heart Bleed
Smarter targeted attacks
Adware
Hactivists
Critical infrastructure attacks
Pharming
War driving
Social media based attacks
Smart device attacks
Identity theft
Zero-day
Spear phishing
Social engineering
Malware
Threat sophistication
Botnets
Virus
Script kiddies
Worms
Phishing
Spyware
Hackers
Organized hackers
Data breach
War dialing
Web attacks
Physical threat
Fraud
Spam
Trojans
Network attacks
Insider threat
Data in Secure Business System Silo
• Mainframe systems
• Siloed information systems
• Emergence of Open Systems
• Internetworking
Internet Access and Highly Connected Systems
• Web-enablement and online access to citizen data
• Advances in internetworking
• Citizen self service
24*7 Access, Mobile, Anywhere & Anytime
• Integrated online eligibility systems
• Cloud computing
• Mobile
• Big data
User Experience Driven; Data Everywheree
• Wearable Technology
• Internet-of-Things
• Drones
• Federated identity for access to government and non-governmental systems
• Artificial intelligence
• Virtual currency (bit coins)
• Mobile Payment
• Smart devices
1990s
2000s
2010 – Now
Near Future





Generative pre-trained transformer

GPT

GPT-4 vs. ChatGPT

Made for good… But…

ZERO TRUST
SOLDIER

ZERO TRUST
SOLDIER

ZERO TRUST
SOLDIER

Ansvar

ZERO TRUST
SOLDIER

ZERO TRUST
SOLDIER

IT ≠ IS

Østre Toten kommune

Snarveier

Koronainformasjon

← Aktuelt

Rapport etter dataangrepet

Grethe Østby, stipendiat ved institutt for informasjonssikkerhet og kommunikasjonsteknologi ved NTNU, har gått igjennom Østre Toten kommunes håndtering av dataangrepet 9. januar i fjor.

NTNU
Kunnskap for en bedre verden

ZERO TRUST
SOLDIER

NASJONAL
SIKKERHETSMYNDIGHET

ZERO TRUST
SOLDIER

Veileder i sikkerhetsstyring

3. Sikkerhetsledelse

Virksomhetens leder har det endelige ansvaret for det forebyggende sikkerhetsarbeidet og for at dette arbeidet gir forsvarlig sikkerhet som resultat. «Virksomhetens leder» må tolkes i lys av ansvarsfordelingen som fremgår av forvaltningsretten for offentlige virksomheter og selskapsretten for private virksomheter. Ansvaret omfatter forebyggende sikkerhetsarbeid i virksomheten og sikkerhetsarbeid knyttet til aktiviteter utført av andre for virksomheten.

Ansvaret innebærer utøvelse av sikkerhetsledelse. Dette omfatter fastlegging av prinsipper for forebyggende sikkerhetsarbeid, fordeling av ansvar og myndighet for gjennomføring av arbeidet, tilrettelegging for slik gjennomføring og oppfølging av det forebyggende sikkerhetsarbeidet.

Sikkerhetsloven stiller krav til sikkerhetsledelse i:

§ 4-1. Sikkerhetsstyring (første ledd første setning)

Virksomhetens leder har ansvaret for det forebyggende sikkerhetsarbeidet.

Styringsdokument for forebyggende sikkerhetsarbeid

Virksomheten har ansvar for [objekt] som iht. sikkerhetsloven er et skjermingsverdig objekt. Objektet er klassifisert som KRITISK. Virksomheten behandler informasjon som er skjermingsverdig iht. sikkerhetsloven skjermingsverdige objektet. Informasjonen er sikkerhetsgradert inntil HEMMELIG.

Objekt og informasjon er sikret iht. krav om sikring av hhv skjermingsverdig objekt og skjermingsverdig informasjon gitt i eller i medhold av sikkerhetsloven.

Ansvar og myndighet for det forebyggende sikkerhetsarbeidet er fordelt slik at ledelsen har det endelige ansvaret for sikkerhetsarbeidet, linjeledere er ansvarlig for sikkerhetsarbeidet innen sitt myndighetsområde og hver medarbeider har ansvar for at egen arbeidsutførelse er sikker og som besluttet. Virksomhetens leder har utpekt en Sikkerhetsleder som bistår i det forebyggende sikkerhetsarbeidet og har særlige oppgaver knyttet til hendelseshåndtering, sikkerhetsrevisjon og ledelsens årlige gjennomgang av arbeidet.

Sikring er etablert med utgangspunkt i skadevurdering og trusselvurdering. Disse vurderingene oppdateres etter behov og minst årlig i form av en helhetlig risikovurdering for virksomheten. I tillegg gjennomføres avgrensede risikovurderinger ved alle endringer – eksterne eller interne – som kan påvirke sikkerheten. De operative risikovurderingene benyttes som grunnlag for valg og etablering av sikkerhetstiltak.

Forbyggende sikkerhetsarbeid gjennomføres som sikkerhetsstyring. Sikkerhetsstyringen er del av virksomhetens samlede virksomhetsstyring og gjennomføres iht. allment akseptert standard for sikkerhetsstyring og NSMs grunnprinsipper for IKT-sikkerhet. Bl.a. gjennomføres jevnlige sikkerhetsrevisjoner og årlige gjennomganger av de forebyggende sikkerhetsarbeidet.

Boks 1: Eksempel på innhold i styringsdokument for forebyggende sikkerhet

Datatilsynet

ZERO TRUST
SOLDIER

Overtredelsesgebyr til Stortinget

Høsten 2020 ble Stortinget utsatt for datainnbrudd, og Datatilsynet varslet i januar et gebyr på to millioner kroner for manglende sikkerhetsnivå. Vi har nå vurdert Stortingets merknader og sendt vedtak der vi opprettholder det varslede gebyret.

– Vår konklusjon er at stortingsadministrasjonen ikke gjennomførte egnede tekniske og organisatoriske tiltak for å oppnå et tilstrekkelig sikkerhetsnivå, sier konstituert direktør Janne Stang Dahl.

STORTINGET

ZERO TRUST
SOLDIER

Hva kan gjøres?

STORTINGET

ZERO TRUST
SOLDIER

ZERO TRUST
SOLDIER

ZERO TRUST
SOLDIER

Kompetanseheving

ZERO TRUST
SOLDIER

ZERO TRUST
SOLDIER

Bevisstgjøring

ZERO TRUST
SOLDIER

Mindset

ZERO TRUST
SOLDIER

Risikovurdering

ZERO TRUST
SOLDIER

ZERO TRUST
SOLDIER

Tjenesteutsetting!?

Krav til leverandør

Må krav:

- Leverandøren må være ISO 27001 sertifisert eller tilsvarende
    - Leverandøren skal levere en SOA, Statement of Applicability
- Leverandøren skal vise dokumentasjon på regelmessig sikkerhetstesting av løsningen
- Det skal være en Shared Security Responsibility Model for klare ansvarsfordelinger
- Uatoriserte innloggingsforsøk skal rapporteres
- Løsningen må ha API støtte for alle funksjoner som er etterspurt i forespørselen
- Kundens SOC skal få logger i sanntid for innlogginger og hendelser til løsningen
- Løsningen må ha kryptering av data ved lagring
- Det skal vises til relevante referansekunder
- Det skal være synlighet på alle administratorer til løsningen, inkludert de fra leverandøren
- Det skal benyttes Multi Faktor Autentisering for alle administratorer
- Løsningen må ha synlighet på bruk av MFA for lokale brukere
- Det skal kjøres backup av løsningen minimum x gang(er) hver dag
- Løsningen skal ha backup for x dager

Bør krav:

- Leverandøren bør vise til en CSA CAIQ besvarelse eller tilsvarende
- Det bør være et beste praksis dokument som forklarer hvordan kunde skal sette opp sin del av løsningen for best sikkerhet
- Det bør eksistere API dokumentasjon
- Det bør overleveres detaljert beskrivelse av løsningen med tanke på isolering fra andre kunder relatert til sikkerhet.
- Hvordan migrere data fra løsningen etter terminering av forhold?
- Er administrasjonsgrensesnittet tilgjengelig fra internett?
- Kundens tenant bør kunne tilgangsbegrenses til å kun kunne nås fra en IP adresse, kundens IP adresse
- Det bør være FIDO2 support for administratorer
- Hvilke sikkerhetssertifiseringer eksisterer for løsningen?
- Hvilken metode benyttes for sikker utvikling av programvare for å redusere sårbarhetene?
- Hvilke utviklingsplaner eksisterer for sikkerhetsfunksjonalitet?
- Hvordan overvåkes løsningen av leverandøren for å avdekke sikkerhetshendelser?
- Hvordan gjøres krypteringsnøkkel håndtering, som rotering?
- Løsningen bør ha en ransomware immutable backup
- Løsningen bør ha en offline backup
- Leverandøren bør vise til krisehåndteringsrutiner og øvelser
- Har leverandøren en MTTR (Mean Time To Recover) definert i timer eller dager?
- Hvordan jobber leverandøren fra et Zero Trust og Assume Breach perspektiv?

ZERO TRUST
SOLDIER

System vs mennesker

Takk for meg!

sikkerhet@gorantomte.com

https://www.linkedin.com/in/gorantomte/