DIGITALISERING OG SIKKERHET

Ved Jan Petter Torgersrud/Datametrix

DIGITALISERING, HVA BETYR DET?

- Min versjon: Det handler om å flytte manuelle arbeidsoppgaver over på et digitalt medium for effektivisering
- Det hevdes at digitalisering handler minst av alt om teknologi. At det handler mest om hvordan mennesker bruker teknologi til å fornye, forenkle og forbedre. Dette fordi digitalisering gjør det mulig å tilby nye og bedre tjenester, som er enkle å bruke, effektive, og pålitelige
- Ender ofte opp med forbedret ”User experience”
- Treffer oss alle. Vi ser og forstår disse endringene. Den digitale grunnmuren er i endring og må forsterkes med sikkerhet
- Rema selger forsikring, konkurransesituasjonen endres drastisk
- Nye muligheter skapes!


What digitalization
cannot do:
BE HUMAN

Logisk

Rasjonell

Fakta

Detaljer

Historikk

Hva

Kontroll

Regler

Korrekt

Følelser

Emosjonell

Intuisjon

Store bildet

Fremtid

Hvorfor

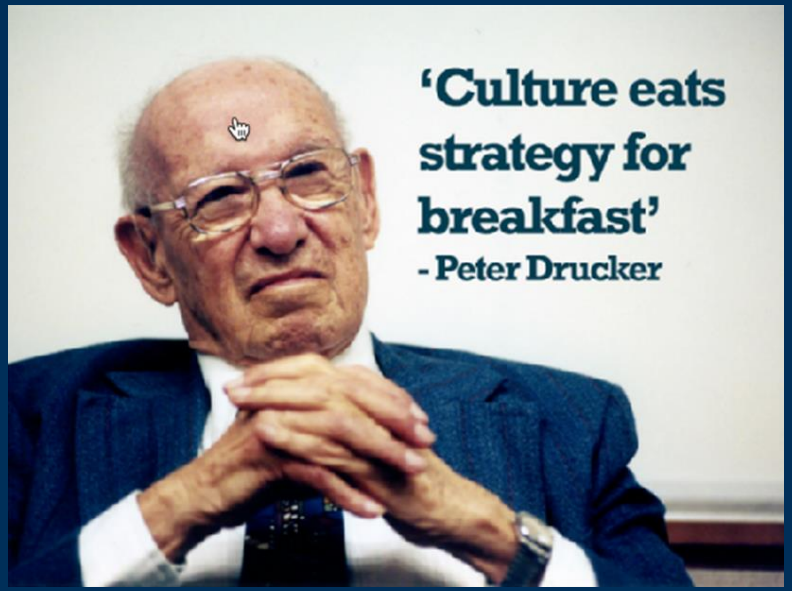
Kreativitet

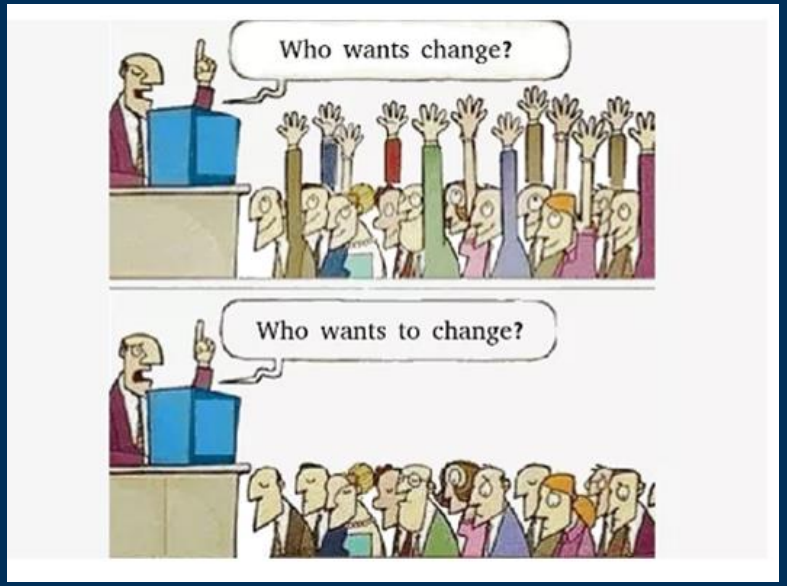
Tenke selv

Empati

MEN, DIGITALISERINGEN GIR ENDRING

- Og med endring vekkes usikkerheten …





- VI HAR BEHOV FOR Å KUNNE JOBBE TRYGGERE
- SIKKERHET 2.0

20 mill

Hver dag skjer det over 20 millioner cyberangrep verden over. Halvparten av cyberangrepene i USA, Europa og midt-Østen er ransomeware angrep *(kilde Checkpoint)*

65%

65% av all e-post er spam. E-post er en primærkanal for spredning av ondsinnet kode. Infiserte zip-filer er mest utbredt, etterfulgt av wordfiler *(kilde Cisco)*

70%

70% av norske respondenter sier at de i stor eller noen grad er bekymret for at norske samfunnskritiske funksjoner skal kunne slås ut av cyberangrep *(kilde Telenor)*

TRE UTBREDTE ANGREPSFORMER

MALWARE

Et virus (program eller algoritme) som kommer inn på endeutstyr og ødelegger filer. Spres gjennom reklame, URL eller pop-up

SPYWARE

Et virus som samler informasjon om en person eller en organisasjon. Kommer inn som programvare, og kan brukes til spionasje

CRYPTOLOCK

Skadelig programvare som infiserer endeutstyr og krypterer filer. Spres via e-post, skadelige lenker eller via ondsinnet kode. Det kreves løsepenger for å dekryptere igjen

HVA GJØR DERE FOR Å SIKRE DERE I ET STADIG ØKENDE TRUSSELBILDE?

Hvordan beskytter dere brukere uansett hvor de jobber fra?

Er det en utfordring å ha god kontroll på bruk av skytjenester?

Hvordan kontrollerer dere hvem som har tilgang til nettet?

Er det en utfordring for dere å ha flere sikkerhets-leverandører?

Har dere opplevd at brukere har blitt utsatt for angrep på sine enheter?

HVA KAN VI GJØRE FOR DEG?

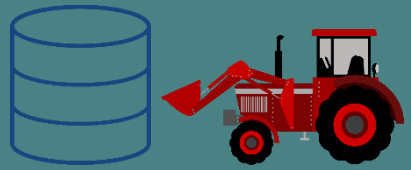
SIKKERHET 2.0

Arkitektur

En helhetlig arkitektur for sikring av kritisk IT Infrastruktur

Automasjon

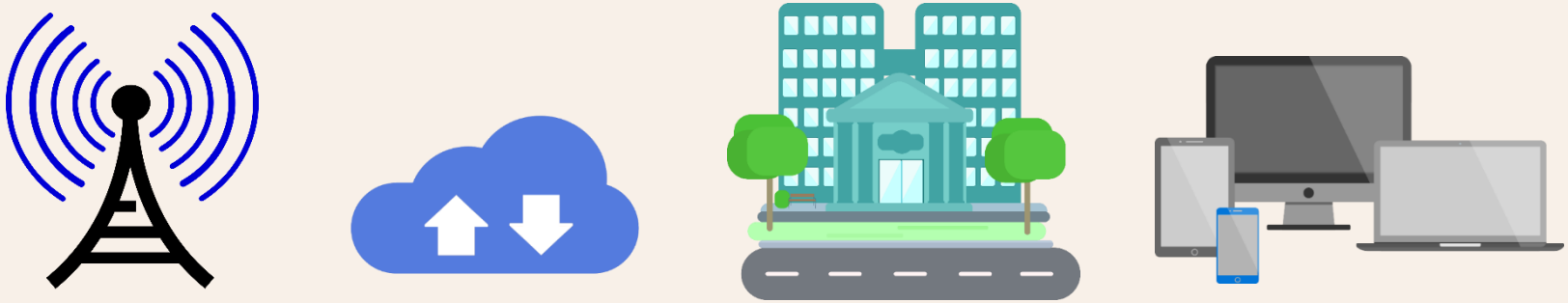
Basert på automasjon og integrasjon



Vi river siloene

For å bygge et helhetlig sikkerhetskonsept på tvers av et fragmentert marked. Vi får nettverk, sikkerhet, programvare og leverandører til å jobbe sammen

SIKKERHETSKONSEPT ENDE-TIL-ENDE



Telecom

Skytjenester/ applikasjoner

Nettverk / infrastruktur

Endepunkter

FRA MOBIL OG ENDEPUNKTER TIL NETTVERK, APPLIKASJONER OG SKYTJENESTER

GLOBAL, NASJONAL OG LOKAL INNSIKT

TALOS

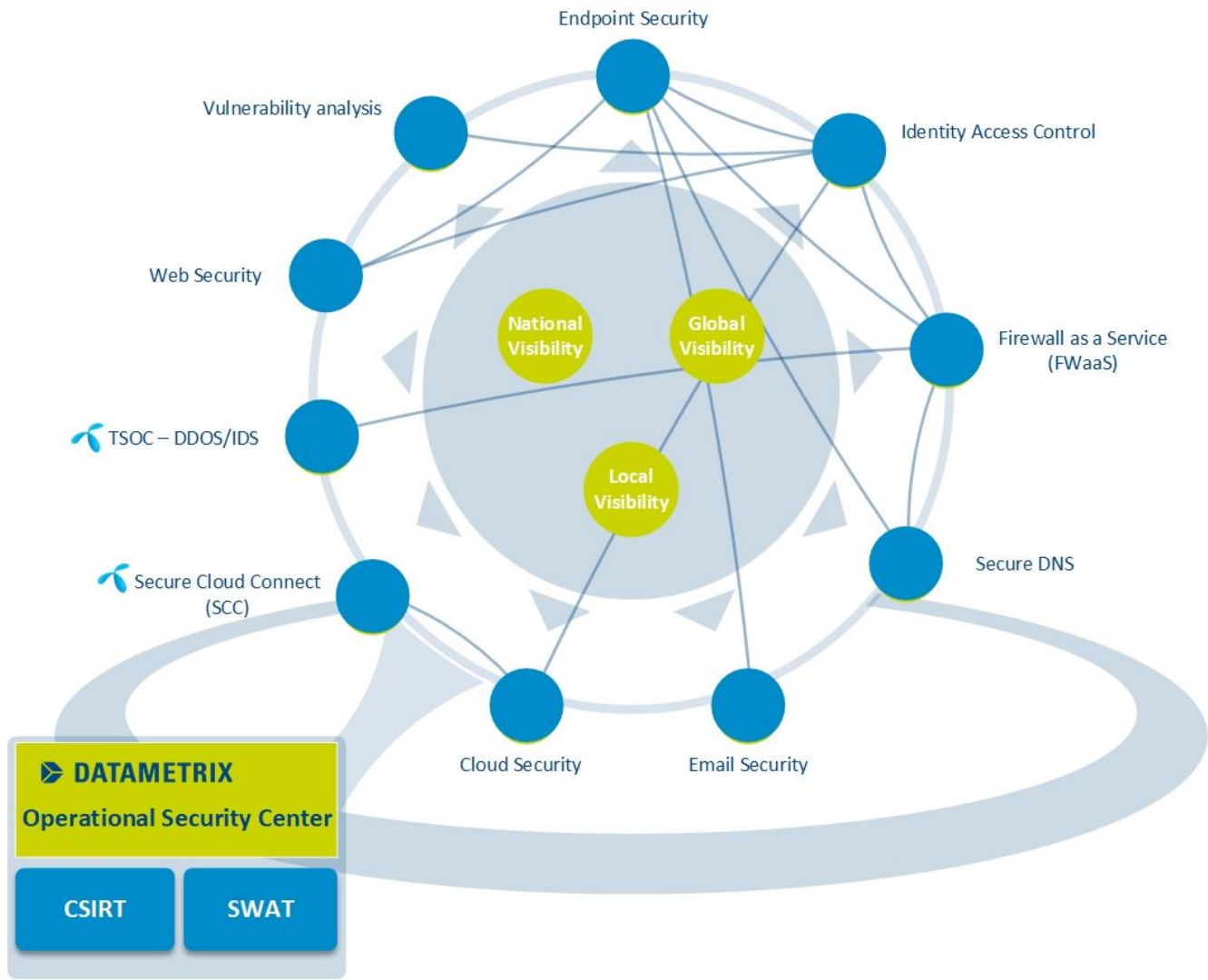
+

TSOC

+

Lokal infrastruktur

= HELHETLIG SIKKERHETSKONSEPT
OPERATIONAL SECURITY CENTER


Endpoint Security
Vulnerability analysis
Identity Access Control
Web Security
National Visibility
Global Visibility
Firewall as a Service (FWaaS)
TSOC – DDOS/IDS
Local Visibility
Secure DNS
Secure Cloud Connect (SCC)
Cloud Security
Email Security
DATAMETRIX
Operational Security Center
CSIRT
SWAT

ET GODT STED Å STARTE

SÅRBARHETSANALYSE

Gir innsikt i bedriftens sårbarhet og eksponering, og bedre forståelse for hvilken risiko man er eksponert for fra internett eller egen infrastruktur.

Tekniker sendes ut og foretar en helsesjekk av nettverk.

Det kan utføres kontinuerlig, automatisert sårbarhetsanalyse av eksponerte tjenester med rapportering

E-POST SIKKERHET

Beskytter innkommende og utgående e-post. Avansert beskyttelse mot sikkerhetsangrep via e-post med hurtig oppdatering og tilpasning.

Kryptering av e-post og beskyttelse mot tap av data. Løsningen er integrert mot Office 365

ENDEPUNKTSIKKERHET

Sikrer endepunkter som PC-er, nettbrett, smarttelefoner og servere. Skal i første rekke beskytte enhetene, men sikrer også nettverket. Man sikrer endepunktene og nettverket ved bruk av VPN, tilgangskontroll og anti-virus programvare

SIKKER DNS

Sikker DNS gir full synlighet over bedriftens internettaktivitet, har mulighet for URL filtrering og blokkerer uønsket aktivitet. Implementering av sikker DNS vil gi brukere beskyttelse mot infisering uansett klient eller protokoll og gi 70% raskere nettsurfing

EN MULIG VEI VIDERE

WEB SIKKERHET

Beskytter ved å automatisk blokkere risikable nettsteder, og tester ukjente nettsteder før brukerne får lov til å koble seg til dem.

Gir beskyttelse før, under og etter et angrep.

Skanner all webtrafikk i sanntid for både kjent og ny malware

BRANNMUR SOM EN TJENESTE

Dette er en brannmur med integrert nettverksplattform som kombinerer en tradisjonell brannmur med en annen nettverksbasert filtrerings-funksjonalitet.

På bakgrunn av automasjon kan den settes opp til å oppdage nye systemer som skal beskyttes og beskytte mot nyoppdagede sårbarheter

SIKKERHET I SKYEN

Beskytter dine brukere, data og applikasjoner, hvor enn de er.

Stopper malware før det når ditt nettverk eller endepunkter, og fjerner usynlige punkter.

Forbedrer sikkerheten uten å påvirke sluttbrukers produktivitet

SIKKER VEI TIL SKYEN

Tjenesten heter Secure Cloud Connect (SCC) og er en forbindelse mellom bedriften og skyleverandører, som ikke går via den ordinære internettrafikken.

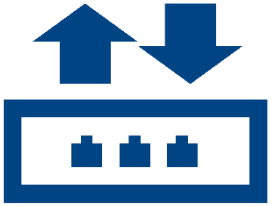
Secure Cloud Connect er tilgjengelig for Nordic Connect kunder

EN MULIG VEI VIDERE

IDENTITETS- OG ADGANGSKONTROLL

Rollebasert tilgang til nettverket. Innstilling av regler basert på bruker, hvorfra og hva slags utstyr brukeren kobles opp med.

Administrasjonsverktøyet logger aktivitet slik at hendelser kan etterforskes



DEKRYPTERING AV DATAPAKKER

Populært kalt Packet Broker.

Dette er rett og slett en mellommann for nettverksovervåkning av trafikk.

SSL (Secure Socket Layer) kryptering er standard teknologi som brukes til å sende privat informasjon. Packet Broker sørger for SSL dekryptering og sender dekrypterte data til monitorering.

TALOS

Bransjeledende gruppe for trusselintelligens.

Ciscos eget overvåknings-senter. De bruker 24/7-tjeneste for overvåkning av sikkerhendelser globalt. Automatisk oppdatering av sikkerhetsmekanismer.

Denne informasjonen tar vi i bruk i vårt Cyber Security Center

TSOC

Telenor SOC (TSOC) er en avdeling i Telenor som driver en 24/7-tjeneste for sikkerhetsovervåking av kunders nettverk.

Der sitter det analytikere som gjør kontinuerlig analyse av uønsket aktivitet på det nasjonale nettet.

Denne informasjonen tar vi i bruk i vårt Cyber Security Center