Hackere og andre digitale trusler

Hva kan vi gjøre med det da?

Årskonferansen 2018 - KS Bedrift

Arthur Gjengstø
Direktør | BDO Sikkerhet og beredskap |BDO Analyse og utredning|
Mobil 481 27 498, mail arthur.gjengsto@bdo.no
18.04.2018

«There are only two types of companies:

Those that have been hacked,
and those that will be.»

Robert Mueller, FBI Direktør 2012

ANBEFALER VI PENETRASJONSTESTER?

- Ja, og det gjør Regjeringen også.
- Meld. St. 38 (2016-2017): *IKT-sikkerhet – Et felles ansvar*.

6.5 Inntrengingstester

Kartlegging og forsøk på inntrenging skjer kontinuerlig mot enheter koblet på internett. Inntrengingstesting er et effektivt tiltak for å avdekke sårbarheter og teste motstandskraften i IKT-systemer. Dette gjøres gjennom målrettet søk, analyse og forsøksvis utnyttelse av sårbarheter, feil og mangler. Sårbarheter i infrastruktur tilknyttet internett kan også utføres ved bruk av kartleggingsverktøy, som for eksempel Allvis NOR (se boks 6.5).

Justis- og beredskapsdepartementet anbefaler bruk av inntrengingstester. En rekke virksomheter har fulgt anbefalingen, og i de aller fleste tilfel-

VERDIER

Finansielle verdier	Person-opplysninger	Forskning og utvikling	Kontrakts-forhandlinger	Sensitive transaksjoner	Know-how	Sikkerhetsgradert informasjon
Detaljert informasjon om bygg og anlegg	Informasjon om kritisk infrastruktur	Relasjoner til andre virksomheter	Informasjon om politiske beslutningsprosesser	Risiko- og sårbarhetsvurderinger	Markeds-strategier	Sensitive kundeopplysninger
Web-sider	PC og telefon	E-post	Operativ evne	Saksbehandlings-systemer	Kunde-databaser	Produksjons-systemer

BDO RISIKOUNDERSØKELSEN

Norske virksomheter er svært redde for dataangrep, men gjør lite for å motvirke at de skal inntreffe.

- Dataangrep er den risikoen virksomhetene vurderer som mest kritisk i tiden fremover.
- Kun 4 av 10 som inkluderer informasjons- og IKT-sikkerhet i sin risikostyring.

Det er også en risiko for at mange undervurderer sine digitale verdier.

- 6 av 10 virksomheter mener de ikke håndterer informasjonsverdier som har et høyere sikkerhetsbehov.

Kvantitativ og kvalitativt	Ca 1500 respondenter
	Dybdeintervjuer
	Tverrsnitt av norsk næringsliv
Fokus på det digitale risikobildet	Kritiske informasjonsverdier
	Digitale sikkerhetshendelser
	Sikkerhetsutfordringer i tiden fremover
Robusthet	Scenarioanalyse
	Bevissthet

SVARET ER IKKE Å STOPPE UTVIKLINGEN

- Digitalisering er positivt
- Telemedisin
- Driftskontrollsystemer
- Droner
- Vi må gripe mulighetene…

… men vi skal passe oss for …

digital sorgløshet

Innbrudd i datasystemene til Helse Sør-Øst

Profesjonelle aktører har brutt seg inn i datasystemene til Sykehuspartner i Helse Sør-Øst. Helseforetaket ser svært alvorlig på saken, og innbruddet er meldt til politiet.

HELSE SØR ØST: Akershus universitetssykehus HF (Ahus) er ett av mange sykehus som er en del av helseforetaket.
FOTO: LARSEN, HÅKON MOSVOLD / NTB SCANPIX

Henriette Mordt
Journalist

Christina Neumann
Journalist

Oppdatert 18.01.2018, kl. 10:30

TLP:AMBER

Overblikk over situasjonen

Birgit ble svindlet for 1,3 millioner

in historie for å advare andre. Foto:

14. juni 2017, kl. 18:39

Morten deler identitet med en kriminell

Kun en tredjedel anmelder ID-tyveri. Manglende tillit til politiet kan være årsaken, viser undersøkelser. Morten Arntun opplevde at en fremmed brukte kortet hans til å kjøpe flybilletter og varer for 22.000 kroner. Politiet henla saken.

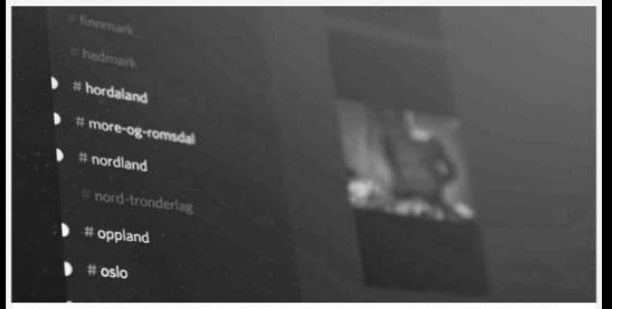
Morten Arntun ble utsatt for identitetstyveri og svindel.
FOTO: AMANDA ÅSBERG / NRK

Amanda Rørmark Åsberg
Journalist

Publisert 20.03.2017, kl. 05:26

FORUM PÅ HEMMELIG APP SPRER SEG OVER HELE LANDET:

Nakenbilder av hundrevis av norske jenter deles på det mørke nettet



FORDELT PÅ FYLKER: Bildene inne på appen er fordelt på fylker. Medlemmene kan også komme med navn på jenter de ønsker bilder av. Foto: Simen Aakjær / TV 2

Petter Stordalens Choice Hotels er blant virksomhetene som er rammet av det internasjonale dataangrepet.
Foto: Terje Pedersen/NTB Scanpix

Nyheter Teknologi

Choice Hotels ble rammet av WannaCry

TUNG TID: Nora Mørk fikk hverdagen snudd på hodet da én person hacket mobiltelefonen hennes og spredde private bilder nettet. Foto Dagbladet

Private bilder av Nora Mørk på avveie

Utga seg for å være direktør: Svindlet festspillene i Nord-Norge for 770.000 kroner

2.400 euro, cirka 770.000 norske kr

Fikk du denne e-posten fra Skatteetaten i dag? Ikke trykk på lenka

Ble du glad da du så eposten fra Skatteetaten der det stod «Vi har funnet ut at du er berettiget til å motta en skatterefusjon 3.950 NOK»? Den er ikke ekte.

Svar Svar til alle Videresend Direktemelding

on 12.07.2017 15:43

Skatteetaten < @ska

Ny melding

Til NRK Rogaland

Syed Ali Shahbaz Akhtar
Journalist

Oppdatert 12.07.2017, kl. 21:01

Kjære kunde,

Vi har funnet ut at du er berettiget til å motta en skatterefusjon 3.950 NOK.
Klikk her for å motta din skatt tilbakebetaling.

NRK har fjernet navnet på avsender. Denne eposten ble sendt til en fellesadresse.
FOTO: SKJERMDUMP / NRK

Nyheter

Også norske bedrifter mål: – Alvorlige dataangrep fra Kina

Ole Peder Gjæver
5. april 2017 15:40 – Oppdatert 6. april 2017 09:28

Del (62) Tweet Epost

Countries targeted

Norge, Sverige og Finland er blant landene den kinesiske hackerligaen APT10 skal ha rammet. Fake[illegible]-rapporten «Operation Cloud Hopper», den offentlige delen av undersøkelsene til PwC UK, BAE Systems og britiske National Cyber Security Cent[illegible]

Sikkerhetstjenesten: Avslørte spionasje-angrep mot norske forskere

HACKET: Kommunikasjonssjef Åsmund Weltzien i NUPI understreker at instituttet har gått grundig gjennom sine sikkerhetssystemer etter spion-angrepet.
FOTO: MATTIS SANDBLAD, VG

Outstanding Security Performance Awards WINNER 2016

«Virksomheter innen norsk forsvars- og beredskapssektor, statsforvaltning, forskning og utvikling samt virksomheter innen kritisk infrastruktur, er å anse som særskilt utsatte etterretningsmål.»

«Innsidere vil i mange tilfeller være etterretningstjenesters beste inngang til skjermingsverdige norske verdier. Dette gjelder blant annet verdier som politiske og økonomiske strategier, teknologi og forskning, registre og sensitive personopplysninger, bank og finans samt informasjon om norsk forsvar, beredskap og kritisk infrastruktur.»

PST (2018): *Trusselvurdering 2018*.

ER 100 % SIKKERHET MULIG?

- Russia hacks Pentagon computers: NBC, citing sources

- NBC News, 6. august 2015

INGEN MAGISK BOKS MED SVAR PÅ ALT

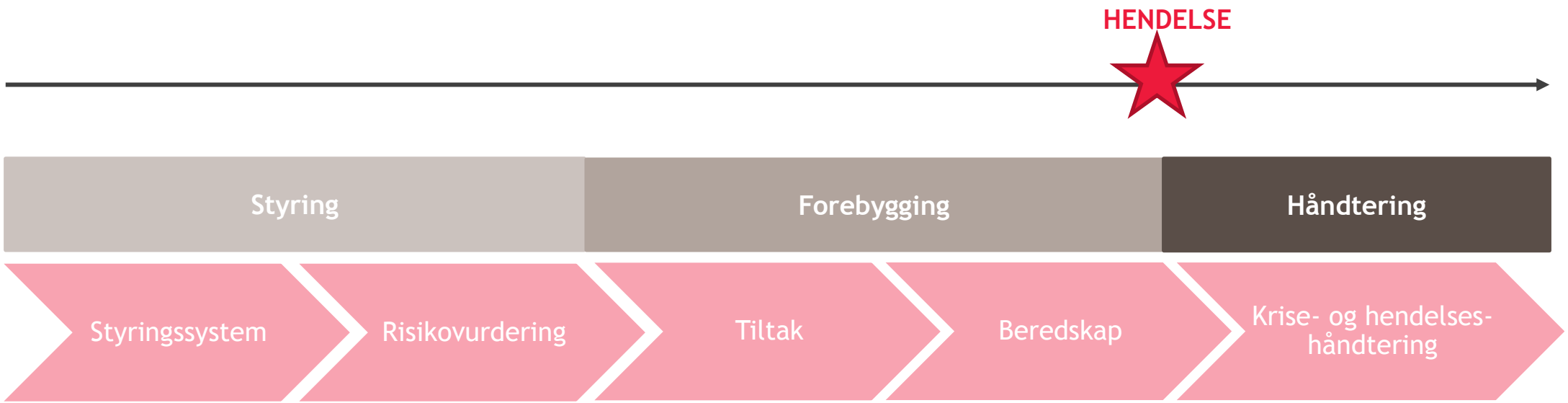
- Trusselen består av motiverte mennesker med stor tilpasningsdyktighet

- 100 % sikkerhet et umulig
- Går an å gjøre mye
- Bør gjøres mer enn i dag

»

Unngå at hackere overtar domenekontrollen før lunsj

TENK HELHETLIG



ER ANTIVIRUS OG BRANNMUR NOK?

BLOKKERT AKTIVITET

LOGGES SELVSAGT

MISLYKKEDE ANGREP

TILLATT AKTIVITET

LOGGES OFTE IKKE

VELLYKKEDE ANGREP

SPØRSMÅL DU SOM LEDER KAN STILLE

- Har vi god nok oversikt over hvilke digitale verdier som vi forvalter?
- Har vi godt kommuniserte mål, policyer og instrukser for å beskytte våre digitale verdier?
- Når gjennomførte vi sist en risikovurdering for å sjekke ut om vi har iverksatt de rette tiltakene for å sikre våre verdier mot relevante trusler? Ble dette forelagt og behandlet i virksomhetsledelsen?
- Stiller vi tydelige krav og gjennomfører revisjoner av våre leverandører av kritiske IT-tjenester?
- Har risikovurderingen konkret tatt for seg våre mest kritiske informasjonssystemer?
- Medførte risikovurderingen av tiltak ble besluttet? Er beslutningene fulgt opp? Hva vet vi om effekten av tiltakene?
- Har vi gjennomført en sikkerhetstest i etterkant for å sjekke ut at sårbarhetene er luket bort?

Er sensitive data og kritiske informasjonssystemer godt nok beskyttet?

Å TA MED SEG HJEM: EKSEMPLER PÅ TILTAK DU BØR VURDERE

1. Sørg for at alle i virksomheten får nok opplæring.
2. Sørg for tydelig definert ansvar, roller og fullmakter innen IT-sikkerhet.
3. Skaff deg oversikt over hvilke digitale verdier du eier, hva som kan true de & hvor sårbar du er.
4. Få gjennomført en risikoanalyse (eller en GAP-analyse) for å identifisere gap mellom «må/bør- og er-situasjon». Sjekk ut både policy, prosesser, planer, prosedyrer og tiltak. Få opp plan og gjør tiltak.
5. Få opp en forstått informasjonssikkerhetspolicy, brukerinstrukser og gode varslingssystemer.
6. Arbeid kontinuerlig med informasjonssikkerhetskulturen i virksomheten.
7. Sjekk ut at det gjennomføres regelmessige sikkerhetstester fra etiske hackere.
8. Påse at virksomheten har en oppdatert og tiltaksorientert beredskapsplan for uønskede hendelser.
9. Sørg for at det med jevne mellomrom gjennomføres øvelser, både strategisk og operativt.
10. Ha fokus på virksomhetens oppfølging av NSMs grunnprinsipper for IKT-sikkerhet (egen slide).

»

Tonen fra toppen

- eksemplets makt

Å TA MED SEG HJEM: UTVIKLE EN SUNN SIKKERHETSKULTUR

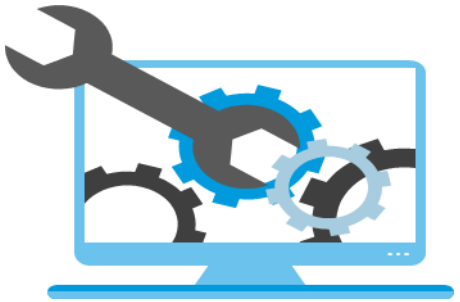
- Å bygge opp en sunn it-sikkerhetskultur er avgjørende for å utvikle virksomhetens sikkerhet, slik at sikkerhet hele tiden er en del av tjenesteutvikling, drift og kundeleveranser.
- Å utvikle en it-sikkerhetskultur demonstrerer at sikkerhet ikke bare er en oppgave for IT-avdelingen, men et viktig ansvar for hele organisasjonen – fra styret til midlertidig ansatte.
- Å utvikle en it-sikkerhetskultur kommuniserer at man trenger alle med, og at alle har et ansvar for å styrke virksomhetens evne til å stå imot trusler.
- IT-sikkerhet er en investering i den enkelte. Det gjør alle mer kompetent til å møte nye utfordringer.

Å TA MED SEG HJEM: TRENING

- Spam, epost-phishing (nettfiske) og bruk av sosial manipulering for å få tak i informasjon utnytter folks godtroenhet og hjelpsomhet.
- Trening av brukerne i å bli bevisst digitale trusler og vite hva man skal gjøre ved uønskede hendelser er kritisk.
- Ansatte som håndterer person- og annen sensitiv informasjon bør regelmessig gjennomføre slik trening.
- Treningen bør ofte inkludere phishing-øvelser og bruk av sosial manipulasjon.
- Test alt som er av back up-systemer og nedetid-prosedyrer ofte.

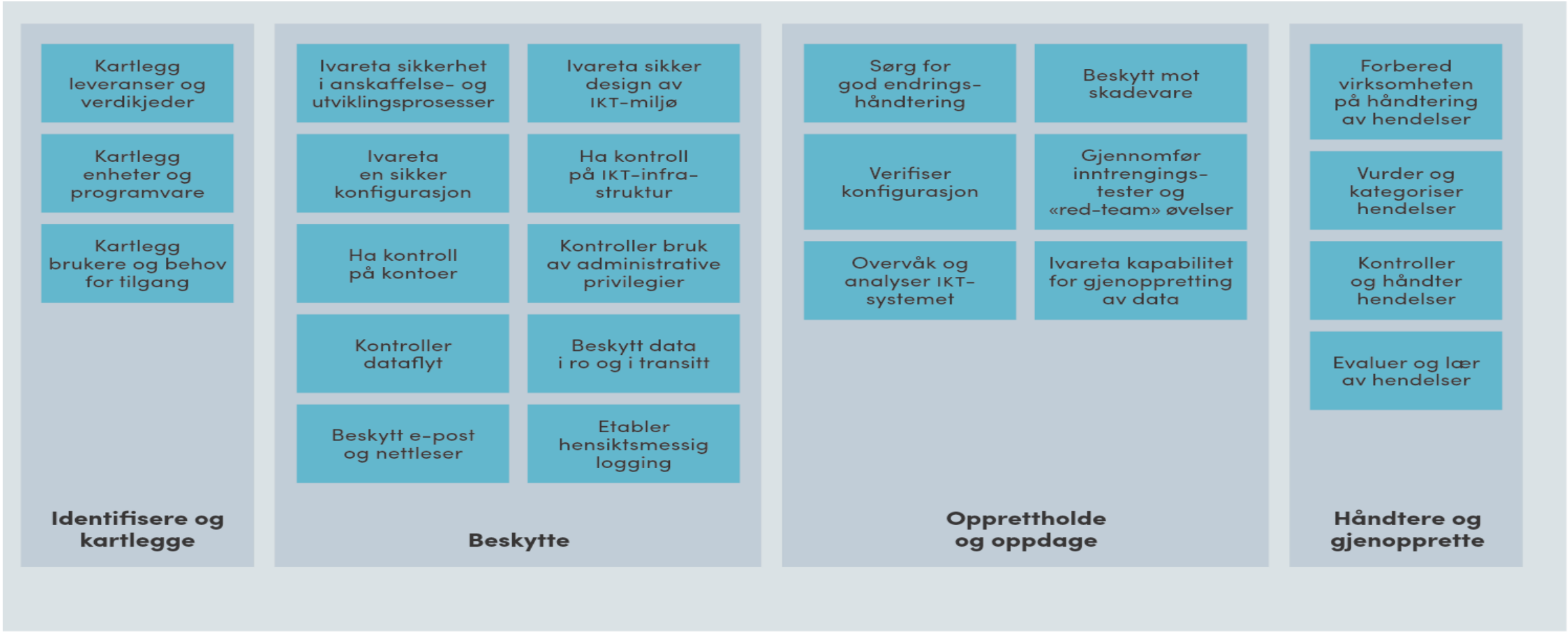
Å TA MED SEG HJEM: OPPFØLGING AV LEVERANDØRER

- Gjennomgå sikkerhets- og beredskapskrav som er satt i avtaler med eksterne.
- Gjennomfør evalueringer av tjenesteleverandørenes ivaretakelse av sikkerhetskrav.
- Sjekk opp at tjenesteleverandørene er bevisste på aktuelle trusler og kontinuerlig følger opp sine egne sikkerhetsprogrammer.



NSM SINE GRUNNPRINSIPPER FOR IKT-SIKKERHET

Kilde: https://nsm.stat.no/globalassets/dokumenter/nsm_grunnprinsipper_ikt-sikkerhet_enkeltside_3008.pdf



»

Regelverket innenfor bl.a. de ulike sektorene

IT-SIKKERHET KREVER ULIKE TYPER AV TILTAK

- God balanse mellom menneskelige, organisatoriske og teknologiske tiltak

- Sikkerhet gjennom holdninger og atferd
  - En god sikkerhetskultur som ledes fra toppen og dyrkes: tren og mobiliser kraften i organisasjonen.
- Sikkerhet gjennom design
  - Risikobaserte forretningsstrategier, god sikkerhetsarkitektur, krav og oppfølging av leverandører.
- Sikkerhet for grunnleggende verdier gjennom kontrollordninger
  - Dette er for eksempel tilgangsstyring, patching og testing.
- Sikkerhet gjennom god beredskap
  - Overvåking av alvorlige hendelser, varsling, back up, beredskapsplaner og hendelseskompetanse.

«There are only two types of companies:

Those that have been hacked,
and those that will be.»

Robert Mueller, FBI Direktør 2012

»

*Det **finnes ingen kvikk-fiks**, men*

*du bør være **proaktiv***

- Det er dyrere å la være -

BDO AS
Vika Atrium
Munkedamsveien 45
0121 Oslo

ARTHUR GJENGSTØ
BDO Sikkerhet og beredskap | BDO Analyse og utredning
Nasjonal bransjeleder for fornybar energi
Mobil +47 481 27 498