Mørketallsundersøkelsen 2020

De 7 anbefalingene

Din tilstand med en helsesjekk

Data Equipment

Gøran Tømte

CISO and Zero Trust soldier

Working to change and enhance. Start with the mindset.

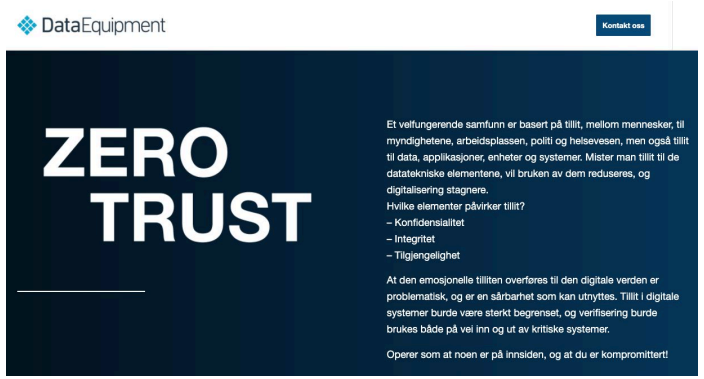
«Suksessfulle hendelser skjer i tillatt trafikk»

Data Equipment

DataEquipment

Vi gjør Norge sikrere

INTELLISEC



CIS Center for Internet Security®

CSA cloud security alliance®

NASJONAL SIKKERHETSMYNDIGHET

DataEquipment paloalto NETWORKS Extreme networks ADVANCE WITH US proofpoint. DUO tenable® aruba a Hewlett Packard Enterprise company thycotic

DataEquipment

Vi gjør Norge sikrere

Why?


APRIL
FOOLS'
DAY


THE UNITED STATES OF AMERICA
ONE DOLLAR

→ Du har alt ansvaret

~~Delt ansvar~~

Næringslivets sikkerhets-råd

Mørketalls-undersøkelsen 2020

Karakteristikker

Respondentene i undersøkelsen har følgende fordeling mellom privat og offentlig sektor:

Sektor	Antall (n)	Andel intervju
Privat	1017	67 %
Offentlig	530	33 %
Totalt	1601	100 %

Virksomhetsstørrelse

Undersøkelsen omfatter virksomheter i følgende størrelsesgrupper.

Virksomhetsstørrelse	Antall intervju	Andel intervju
5 til 19 ansatte	844	52,7 %
20 til 99 ansatte	537	33,5 %
100 ansatte eller flere	220	13,7 %
Totalt	1601	100 %

Bransje

Undersøkelsen omfatter virksomheter i følgende bransjer.

Bransje	Antall	Andel intervju
Primær	14	0,9 %
Industri etc.	148	9,2 %
Bygg- og anleggsvirksomhet	112	7,0 %
Varehandel etc.	411	25,7 %
Transport og lagring	42	2,6 %
Overnattings- og serverings-virksomhet	41	2,6 %
Tjenesteytende næringer	271	16,9 %
Offentlig administrasjon	103	6,4 %
Undervisning	177	11,1 %
Helse og sosial	250	15,6 %
Kulturell virksomhet	32	2,0 %
Totalt	1601	100,0 %

1.1. Outsourcing
1.2 Styringssystem og rammeverk

2.1 Informasjonssikkerhetshendelser
2.2 Hendelser med negative konsekvenser

3. 1 Hvorfor sikkerhetsbrudd oppsto
3.2 Hvordan sikkerhetsbruddet ble oppdaget

4.1 Følger av hendelser
4.2 Rapportering
4.3 Hendelsens kostnad

5.1 Endringer som følge av GDPR
5.2 Opplevd brudd på personopplysningssikkerheten
5.3 Økt bevissthet rundt sikkerhet blant ansatte


Malware
Datainnbrudd
filer
Mistet
OG
hjemmesiden
Ddosangrep
noen
fikk
ikke
Serverkrasj
et
Tyveri
inn
Virus
på
TIL
Det
Innbrudd
som
hos
data
tok
phishing
penger
systemet
ansatt
en
Spam
Svindelforsøk
mail
svindel
datafiler
åpne
har
Nedetid
TILGANG
gdpr
Hacking
BLE
Tap
var
Løsepengesak
Ansatte
om
INFORMASJON
av
å
feil
PC
forsøk
angrep
system
KUNDE
Passord
epost
seg
server
Kryptovirus
bedrageri
Sensitivinfo
skulle
Direktør
brudd
kom
DE
hacket
Misbruk
Virusmail
hjemmesida
Fellesdokumenter
Feilkonfigurasjon
datamaskiner
hendelse
Brukerfeil
Underslag
SYSTEMFEIL
INTERN
Kryptertserver
FEILTAGELSE
Direktørsvindel
autorisert
bærbare
fremme
Phisingforsøk
Outsorceleverandør
Eposthacking
Lekkasje
Svindelsforsøk
Feilsendt
abonnoment
Systemkræsj
Trojansk
låse
Tapt
SLETTET
FØRTE
vårt
Datatap
rutiner
Feilsending
suport
programvare
Drift
tid
Tjenesteavbrudd
nettet
den
UT
link
med
arbeidsdokument
løspenger
avveie
BREV
overføring
betale
ansattes
SENDE
Windows
BRUKT
TILGANG
DEL
kontroll
alle
Utdatert
sindel
Koblet
varc
bedrag
Utskrift
Løsepengesak
adresser
blokkerttrusler
Serverinnbrudd
innloggingsinformasjon
bytte
personopplysning
arbeid
kort
blitt
skrivtlig
sertifikat
odelagt
krevde
hadde
hjemmeside
slettede
adressene
SVARTELISTET
datamaskingserver
nettverk
nettverket
kommet
Kjeling
Ddos
Svindelsforsøk
Feilsendt
email
infisering
abonnoment
Eposthacking
Lekkasje
Outsorceleverandør
rettet
gitt
masse
oppgradering
dokumenter
låste
bytett
KUNDER
mailen
avveie
BREV
løspenger
infisert
vekke
program
misbrukte
locker
sindel
tilgjengelige
Nedetid
Tap
var
Løsepengesak
adresser
Utskrift
Phisingforsøk
skrivtlig
stedfortredere
angående
sertifikat
odelagt
Virusmail
hjemmesida
Fellesdokumenter
Feilkonfigurasjon
kommet
nettverket
Brukerfeil
Underslag
SYSTEMFEIL
INTERN
Kryptertserver
FEILTAGELSE
datamaskiner
hendelse
Direktørsvindel
autorisert
bærbare
fremme
hjemmeside
slettede
adressene
SVARTELISTET
Misbruk
brudd
kom
DE
hacket
Direktør
Sensitivinfo
skulle
Kryptovirus
bedrageri
Serverinnbrudd
innloggingsinformasjon
Passord
epost
seg
server
Ansatte
om
INFORMASJON
av
å
feil
PC
forsøk
angrep
system
KUNDE
TILGANG
gdpr
Hacking
BLE
Tap
var
Løsepengesak
Svindelforsøk
mail
svindel
datafiler
åpne
har
Nedetid
ansatt
en
Spam
phishing
Innbrudd
som
hos
data
tok
Tyveri
inn
Virus
på
TIL
Det
Serverkrasj
et
Ddosangrep
noen
fikk
ikke
Malware
Datainnbrudd
filer
Mistet
OG
hjemmesiden
gikk
switch
overførsel
sviktet
elever
penger
systemet
Datatap
rutiner
suport
programvare
Drift
tid
Tjenesteavbrudd
nettet
den
UT
link
med
arbeidsdokument
overføring
betale
ansattes
SENDE
Windows
BRUKT
TILGANG
DEL
kontroll
alle
Utdatert
sindel
Koblet
varc
bedrag
Utskrift
Løsepengesak
adresser
blokkerttrusler
Serverinnbrudd
innloggingsinformasjon
bytte
personopplysning
arbeid
kort
blitt
skrivtlig
sertifikat
odelagt
krevde
hadde
hjemmeside
slettede
adressene
SVARTELISTET
datamaskingserver
nettverk
nettverket
kommet
Kjeling
Ddos
Svindelsforsøk
Feilsendt
email
infisering
abonnoment
Eposthacking
Lekkasje
Outsorceleverandør
rettet
gitt
masse
oppgradering
dokumenter
låste
bytett
KUNDER
mailen
avveie
BREV
løspenger
infisert
vekke
program
misbrukte
locker
sindel
tilgjengelige
Nedetid
Tap
var
Løsepengesak
adresser
Utskrift
Phisingforsøk
skrivtlig
stedfortredere
angående
sertifikat
odelagt
Virusmail
hjemmesida
Fellesdokumenter
Feilkonfigurasjon
kommet
nettverket
Brukerfeil
Underslag
SYSTEMFEIL
INTERN
Kryptertserver
FEILTAGELSE
datamaskiner
hendelse
Direktørsvindel
autorisert
bærbare
fremme
hjemmeside
slettede
adressene
SVARTELISTET
Misbruk
brudd
kom
DE
hacket
Direktør
Sensitivinfo
skulle
Kryptovirus
bedrageri
Serverinnbrudd
innloggingsinformasjon
Passord
epost
seg
server
Ansatte
om
INFORMASJON
av
å
feil
PC
forsøk
angrep
system
KUNDE
TILGANG
gdpr
Hacking
BLE
Tap
var
Løsepengesak
Svindelforsøk
mail
svindel
datafiler
åpne
har
Nedetid
ansatt
en
Spam
phishing
Innbrudd
som
hos
data
tok
Tyveri
inn
Virus
på
TIL
Det
Serverkrasj
et
Ddosangrep
noen
fikk
ikke
Malware
Datainnbrudd
filer
Mistet
OG
hjemmesiden
gikk
switch
overførsel
sviktet
elever
penger
systemet
Datatap
rutiner
suport
programvare
Drift
tid
Tjenesteavbrudd
nettet
den
UT
link
med
arbeidsdokument
overføring
betale
ansattes
SENDE
Windows
BRUKT
TILGANG
DEL
kontroll
alle
Utdatert
sindel
Koblet
varc
bedrag
Utskrift
Løsepengesak
adresser

1. **Beskytt e-post og nettleser**
   Flere forebyggende tekniske tiltak beskytter transport av e-post mellom servere for å redusere risiko for brudd på konfidensialitet, integritet og e-postmeldinger med falsk avsenderadresse. Disse tiltakene er beskrevet under grunnprinsipp 2.8 «Beskytt e-post og nettleser».

2. **Bruk skadevareskanning på e-postmeldinger og vedlegg**
   Bruk automatiserte verktøy for å analysere innkommende meldinger, meldingsvedlegg og klikkbare lenker i disse for å avdekke skadevare og andre trusler. Dette er beskrevet i tiltak 3.1.3 under grunnprinsipp 3.1 «Oppdag og fjern kjente sårbarheter og trusler».

3. **Merk usikre/mistenkelige meldinger**
   Det kan være til hjelp for brukerne dersom meldinger er tydelig merket dersom de ikke har vært sikret under transport mellom servere som beskrevet i punkt 1 av denne listen, eller dersom de er identifisert som mistenkelige av tiltaket som er beskrevet i punkt 2 av denne listen.

4. **Autentisering av brukere**
   En trusselaktør kan også skaffe seg adgang til e-postsystemet ved å utnytte en brukers tilgang og sende meldinger med skadevare fra den interne brukeren. På denne måten kan trusselaktøren omgå noen av de forebyggende sikkerhetstiltakene som er nevnt over i denne listen. NSMs grunnprinsipp 2.6 «Ha kontroll på identiteter og tilganger» beskriver relevante tiltak.

5. **Gi brukere opplæring og bedre risikoforståelse**
   Selv om det er etablert flere lag med forebyggende tekniske sikkerhetstiltak er det risiko for at meldinger med skadevare eller manipuleringsangrep havner i brukerens innboks. Sosial manipulasjon fungerer. Da er det viktig at brukerne har fått opplæring og har en sikkerhetsforståelse som reduserer risikoen for at de lar seg lure.

6. **Oppdag sikkerhetsbrudd**
   For trusselaktøren er det bare et spørsmål om tid. Uansett hvor mange lag med forebyggende sikkerhetstiltak som er etablert kan sikkerhetshendelser ramme alle virksomheter. Da er det vesentlig å ha etablert gode og effektive konsekvensreduserende tiltak. Rask deteksjon av sikkerhetsbrudd er det beste utgangspunktet for å redusere konsekvensene av et sikkerhetsbrudd. Grunnprinsippene 3.2 «Etabler sikkerhetsovervåkning» og 3.3 «Analyser data fra sikkerhetsovervåkning» beskriver relevante tiltak som kan etableres for å oppdage sikkerhetsbrudd.

7. **Håndter hendelser og gjenopprett normal driftssituasjon**
   Det siste punktet i gjennomgangen av scenarioer er håndtering av den uønskede hendelsen. Det gir mulighet til å forberede seg på mulige hendelser med en målsetning om at håndtering av denne typen hendelser kan gjennomføres effektivt. NSMs grunnprinsipper i kategori 4 «Håndtere og gjenopprette» om å håndtere ønskede hendelser, minimalisere skaden, fjerne hendelsesårsaken og gjenopprette integriteten til nettverk og IKT-systemer.

Ransomware

Direktørsvindel

Phishing

Helsesjekk

NASJONAL SIKKERHETSMYNDIGHET

Hjem Veiledning Test Om

baerum.kommune.no Sjekk

DMARC

Domenenavnet har en DMARC-oppføring.

```
v=DMARC1;p=none;pct=100;rua=mailto:postmaster@baerum.kommune.no;
```

SPF

Domenenavnet har en SPF-oppføring.

```
v=spf1 mx ip4:193.161.44.20/32 ip4:193.161.44.32/32 a:mail.baerum.kommune.no a:mail2.baerum.kommune.no a:smtp.onevoice.no a:msg-out.onevoice.no include:_vaspf.fxh42.net include:spf.protection.outlook.com -all
```

MX TOOLBOX

Pricing Tools Delivery Center

SuperTool MX Lookup Blacklists DMARC Diagnostics Email Health DNS Lookup Analyze Headers

SuperTool Beta7

baerum.kommune.no DMARC Lookup

dmarc:baerum.kommune.no Find Problems Solve Email Delivery Problems dmarc

```
v=DMARC1;p=none;pct=100;rua=mailto:postmaster@baerum.kommune.no;
```

Tag	TagValue	Name	Description
v	DMARC1	Version	Identifies the record retrieved as a DMARC record. It must be the first tag in the list.
p	none	Policy	Policy to apply to email that fails the DMARC test. Valid values can be 'none', 'quarantine', or 'reject'.
pct	100	Percentage	Percentage of messages from the Domain Owner's mail stream to which the DMARC policy is to be applied. Valid value is an integer between 0 to 100.
rua	mailto:postmaster@baerum.kommune.no	Receivers	Addresses to which aggregate feedback is to be sent. Comma separated plain-text list of DMARC URIs.

	Test	Result	
!	DMARC Policy Not Enabled	DMARC Quarantine/Reject policy not enabled	More Info
✓	DMARC Record Published	DMARC Record found	
✓	DMARC Syntax Check	The record is valid	
✓	DMARC External Validation	All external domains in your DMARC record are giving permission to send them DMARC reports.	
✓	DMARC Multiple Records	Multiple DMARC records corrected to a single record.	

Data Equipment

NASJONAL SIKKERHETSMYNDIGHET

Hjem Veiledning Test Om

niklas.host Sjekk

DMARC

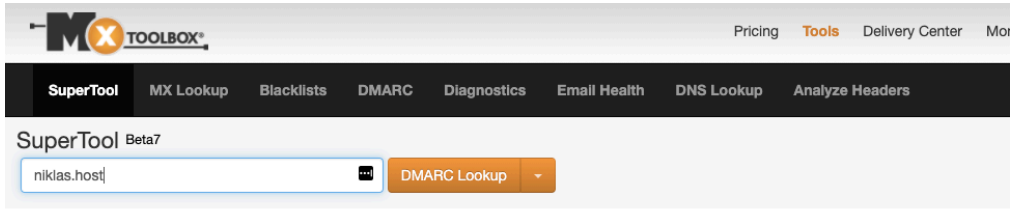
Domenenavnet har en DMARC-oppføring.

`v=DMARC1 Denne gikk ikke helt etter planen eller hva NSM?`

SPF

Domenenavnet har en SPF-oppføring.

`v=spf1 Alle barna validate SPF korrekt utenom NSM, de hadde dratt hjem...`



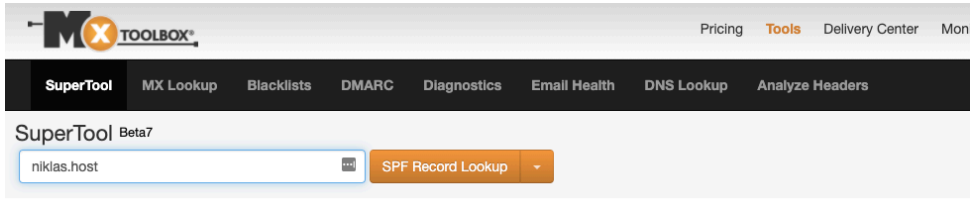
dmarc:niklas.host Find Problems Error

EMAILS BOUNCING? MxToolbox has your email delivery solutions

`v=DMARC1 Denne gikk ikke helt etter planen eller hva NSM?`

Tag	TagValue	Name	Description	Error
v	DMARC1 Denne gikk ikke helt etter planen eller hva NSM?	Version	Identifies the record retrieved as a DMARC record. It must be the first tag in the list.	V: It MUST have the value of 'DMARC1' (all capitals)
p		Policy	Policy to apply to email that fails the DMARC test. Valid values can be 'none', 'quarantine', or 'reject'.	Required tag not found

	Test	Result	
✗	DMARC Syntax Check	The record is not valid	More Info
✓	DMARC Record Published	DMARC Record found	



spf:niklas.host Find Problems Error

EMAILS BOUNCING? MxToolbox has your email delivery solutions

`v=spf1 Alle barna validate SPF korrekt utenom NSM, de hadde dratt hjem...`

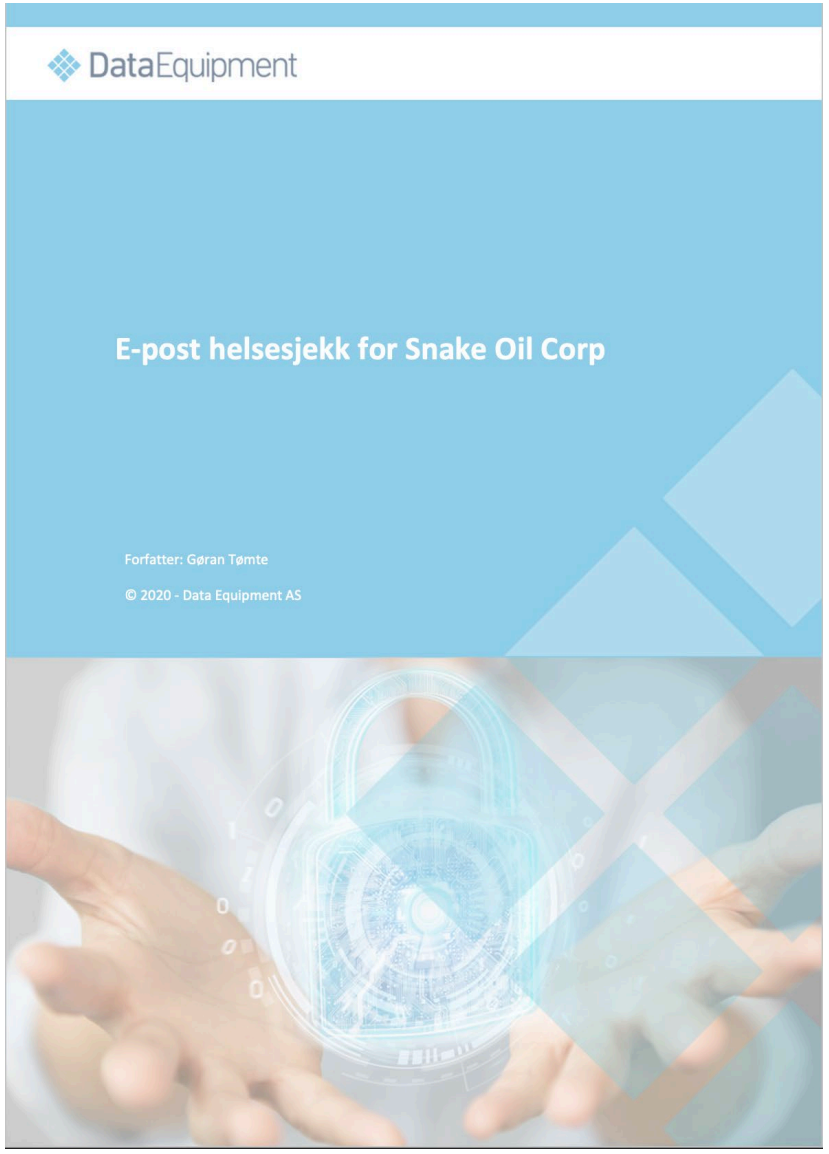
Prefix	Type	Value	PrefixDesc	Description	Error
	v	spf1		The SPF record version	
+	Alle		Pass	Unknown	Unknown mechanisms are not allowed
+	barna		Pass	Unknown	Unknown mechanisms are not allowed
+	validate		Pass	Unknown	Unknown mechanisms are not allowed
+	SPF		Pass	Unknown	Unknown mechanisms are not allowed
+	korrekt		Pass	Unknown	Unknown mechanisms are not allowed
+	utenom		Pass	Unknown	Unknown mechanisms are not allowed
+	NSM,		Pass	Unknown	Unknown mechanisms are not allowed
+	de		Pass	Unknown	Unknown mechanisms are not allowed
+	hadde		Pass	Unknown	Unknown mechanisms are not allowed
+	dratt		Pass	Unknown	Unknown mechanisms are not allowed
+	hjem...		Pass	Unknown	Unknown mechanisms are not allowed

	Test	Result	
✗	SPF Syntax Check	Invalid syntax found	More Info
!	SPF Contains characters after ALL	Items present after 'ALL'. These will be ignored.	More Info
✓	SPF Record Published	SPF Record found	
✓	SPF Record Deprecated	No deprecated records found	
✓	SPF Multiple Records	Less than two records found	

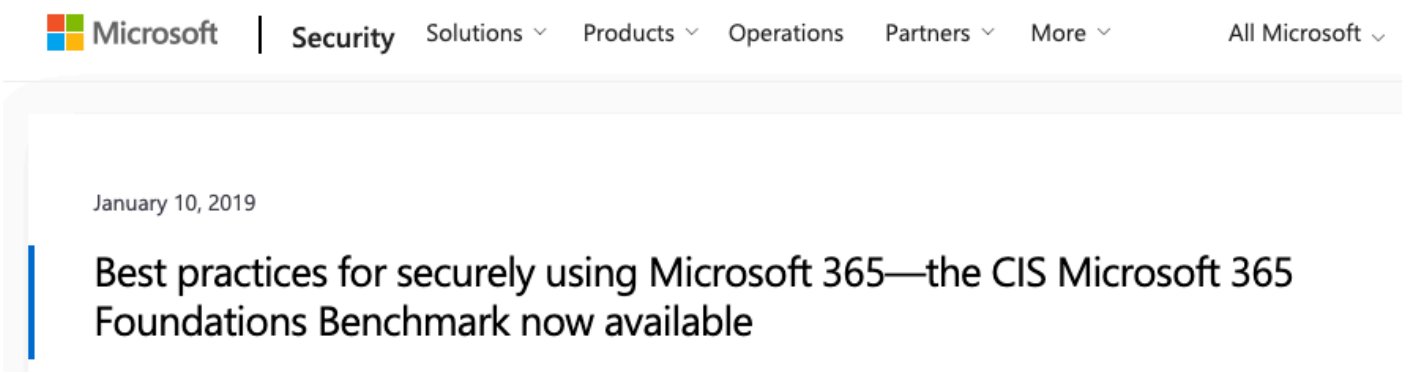
DataEquipment

1. Beskytt e-post og nettleser		Ja	Nei	Delvis	Vet ikke
Flere forebyggende tekniske tiltak beskytter transport av e-post mellom servere for å redusere risiko for brudd på konfidensialitet, integritet og e-postmeldinger med falsk avsenderadresse. Disse tiltakene er beskrevet under grunnprinsipp 2.8 «Beskytt e-post og nettleser».					
Spørsmål:		Ja	Nei	Delvis	Vet ikke
Har du kontroll på alle domener i deres eierskap? Dette er viktig for renomme og omdømme				x	
Er SPF, DKIM og DMARC etablert for alle disse? https://dmarc.no/				x	
Kjøres det kontroll av innkommende e-post opp mot myndighetenes anbefalte sikkerhetsmekanismer som DMARC, SPF, DKIM?			x		

Rapport


DataEquipment
E-post helsesjekk for Snake Oil Corp
Forfatter: Gøran Tømte
© 2020 - Data Equipment AS


CIS Benchmarks™
Securing Microsoft Office
An objective, consensus-driven security guideline for the Microsoft Office Desktop Software.


Microsoft | Security
Solutions
Products
Operations
Partners
More
All Microsoft
January 10, 2019
Best practices for securely using Microsoft 365—the CIS Microsoft 365 Foundations Benchmark now available

Takk for deltakelsen

zerotrust@zerotrust.no

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