

Cyber- og informasjonssikkerhet i Møre og Romsdal



Terje Vernholt

Senior Manager | **Cyber Security**



Cyber- og informasjonssikkerhet i Møre og Romsdal

50 norske virksomhetsledere, IT-ledere og sikkerhetsspesialister har delt sine tanker om ulike forhold knyttet til cyberkriminalitet. De har besvart spørsmål knyttet til blant annet ledelsens involvering i virksomhetens sikkerhetsarbeid og i hvilken grad de er klare til å etterleve kravene til GDPR - EUs nye personvernforordning som trer i kraft 25. mai 2018.





Resultater og refleksjoner

Cybertrusselen bekymrer flere i Møre og Romsdal enn tidligere



59 %

av respondentene er mer **bekymret for trusselen** fra cyberkriminalitet nå, enn det de var for 12 måneder siden



47 %

rapporterer at deres virksomhet har vært **utsatt for én eller flere hendelser** relatert til cybersikkerhet i løpet av forrige regnskapsår



40%

av globale ledere er **bekymret for hvilken innvirkning cyberkriminalitet** vil ha for deres videre vekst og velstand.

Organisert kriminalitet og ansattes ubevisste handlinger er en farlig kombinasjon



39% Organisert kriminalitet



14% Hacktivist



29% Ansattes ubevisste handlinger



12% Mangel på forståelse for cybercrime hos ledelsen



22% Ny teknologi



10% Ansattes bevisste handlinger



20% Lover og regulatoriske krav (feks GDPR)

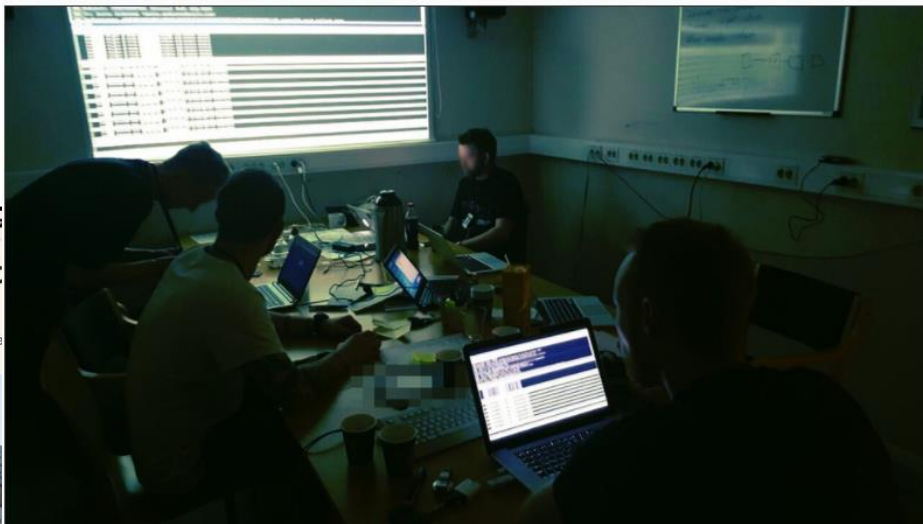


6% Nasjonal kriminalitet

Det vi hører om

Bedragerne lurte ansatt til å utbetale en halv milliard kroner

- Oslo-politiet har samarbeidet med FBI
- Ingen pågrepet så langt



E24 OSLO 10.42 -0.06% OLE 14.43 -0.15% SAP 161.63 EURO 1.11 DOLLAR 2.18

Mærsk Line-sjef: Vi kan ikke t nye ordrer

A.P. Møller-Mærsk har stengt ned enkelte av konsernets IT-systemer i et stoppe at tirsdays hackerangrep sprer seg ytterligere.

```

[REDACTED] your important files are decrypted
If you see this text, then your file are no longer accessible, because they have been encrypted. Perhaps you are being looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption services.
We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.
Please follow the instructions:
1. Send $300 worth of Bitcoin in following address:
1Mz71539mWtR2R1176wS6vAR8B8K
2. Send your Bitcoin wallet ID and personal installation key to e-mail:
www.tb12345@posteo.net. Your personal installation key:
fCbMkH-eomCp-39fDL-36G6C2-yuM6b-WY9K7-35K66-92277-897107-E2208
If you already purchased your key, please enter it below:
key:
    
```

© 2017 Politiet. VS-00 - 18.06.2017 Oppsett: 16.00 - 28.04.2017



Innrømmer at utenlandske IT-tilgang til sensitive pasientdata

arbeidere i Asia og Øst-Europa hatt tilgang og de Ser-Øst, viser informasjon NRK har ut pasientdata til 2,8 millioner nordmenn.



Anne Cecilie Remen
Journalist

Lise Tomter
Journalist

Oppdatert 03.05.2017, kl 10:23

Det er et stort problem. Over 2,8 millioner nordmenn har fått ut sensitive pasientdata som skal driften av infrastrukturen bygges ut til utlandet.

Det vi ikke hører så mye om

Stjålet teknologi havner i Kina

Kinesiske Sixing Liu ble domt for å lekke sensitiv høyteknologi til Ki er blant 100 personer er som mistenkt for å lekke digitale forsvarshemmeligheter.



FOTO: Reuters
Aviskantska myndigheter Internettørn nå kampen mot tryk av sensitive data

Stjeler kontrakter, tegninger, passord og hemmelige data

Ti datainnbrudd er oppdaget i norske selskaper innen forsvar, olje og energi. Dette er den største dataspionasjesaken som er avdekket i Norge. - Meget alvorlig, sier en PST-sjef.



FOTO: OLAW OLSEN
PST har fått innlevert et stort antall dokumenter og data som er mistenkt for å være sensitive data

PST etterforsker dataangrepet mot Helse sørøst som mulig etterretningsvirksomhet

PST mistenker at noen til fordel for fremmed stat står bak nettverksangrep mot Helse sørøst.



FOTO: Varfjell, Fredrik / Scanpix

Tidligere cybersjef vil ha mer åpenhet om dataangrep

Roar Sundseth mener NSM bør offentliggjøre informasjon om dataangrep sendt til bedrifter.

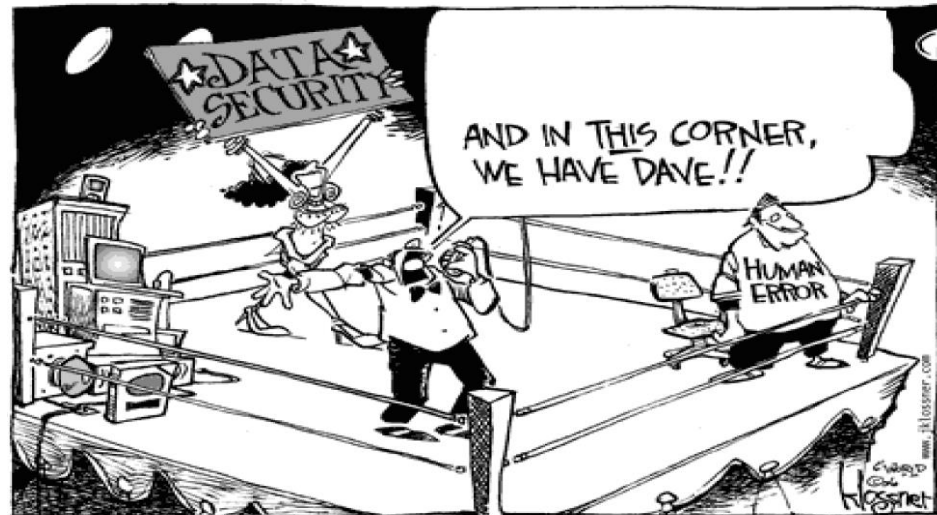
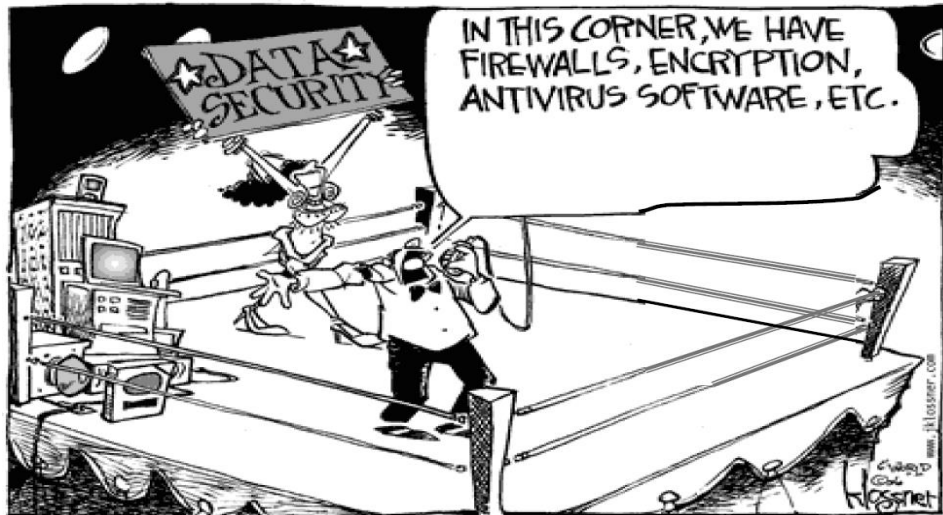


FOTO: Aa. Enevoldt/NTB scener
Roar Sundseth jobber nå i Watchcom, dette bildet er fra 2012.

Spionasje mot norsk industrigigant

- Vi ble utsatt for et avansert, målrettet angrep utført av aktører med store ressurser, sier HR-direktør og sikkerhetsansvarlig, Torild Bugge i Ulstein Group.





Cyberangrep skaper alvorlige konsekvenser for de som rammes

Finansiell svindel



39%

har vært utsatt for **finansiell svindel** de siste 12 månedene

Phishing



35%

har vært utsatt for **phishing-angrep**

Ransomware



18%

har vært utsatt for **ransomware**

Ledelsen må involveres i virksomhetens sikkerhetsarbeid



12%

mener at ledelsen i høy grad har fokus på å oppnå riktig balanse mellom **truslene organisasjonen står overfor** og virksomhetens investeringer i cybersikkerhet



29%

av sikkerhetsansvarlige **informerer aldri ledelsen** om mulig cybertrusler virksomheten står overfor



12%

oppfatter **mangel på ledelsens forståelse** for cyberkriminalitet som **en trussel** mot deres virksomhet de neste 12 månedene.

Er ledelsen ansvarlig for Cyber Security?

Halvparten har ikke en plan for hva de skal gjøre hvis de utsettes for cyberangrep



Styreleder Ann-Kristin Olsen i Helse sør-øst har rekruttert et styre til Sykehuspartner med solid erfaring som helsebyråkrater. Foto: Onsjøen, Ole Gunnar

Nyheter Helse

Helse sør-øst bytter ut styret i Sykehuspartner

Styret i Helse sør-øst har besluttet å skifte ut alle de eieroppnevnte styremedlemmene i datterselskapet Sykehuspartner etter IT-skandalen.

Target CEO Gregg Steinhafel resigns in wake of customer data breach

Chief executive out after 35 years at retail company . Data breach affected 110 million customers

Dominic Rushe in New York
Monday 5 May 2014 13:40 BST

Target's chairman and chief executive resigned on Monday, in the wake of a mass data breach that compromised personal details of some 110 million shoppers.

Gregg Steinhafel, who had been with the retailer for 35 years, had been chief executive since 2008. He will be replaced by John Mulligan, chief financial officer. In February, Mulligan apologised to Congress for the breach.

"The last several months have tested Target in unprecedented ways," Steinhafel said in a statement. "We have already begun taking a number of steps to further fortify our data security, putting the right people, processes and systems in place.

"With several key milestones behind us, now is the right time for new leadership



Equifax/YouTube

Richard Smith will "retire" as chairman of the board and CEO effective September 26.

ve data



pwc.no/cyber



This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PwC AS, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2017 PwC. All rights reserved. In this document, "PwC" refers to PricewaterhouseCoopers AS, which is a member firm of PricewaterhouseCoopers International Limited, each member firm of which is a separate legal entity.