POLITIET
KRIPOS

Politiets rolle og etterforskning ved datainnbrudd

Mathilde Bouyssou

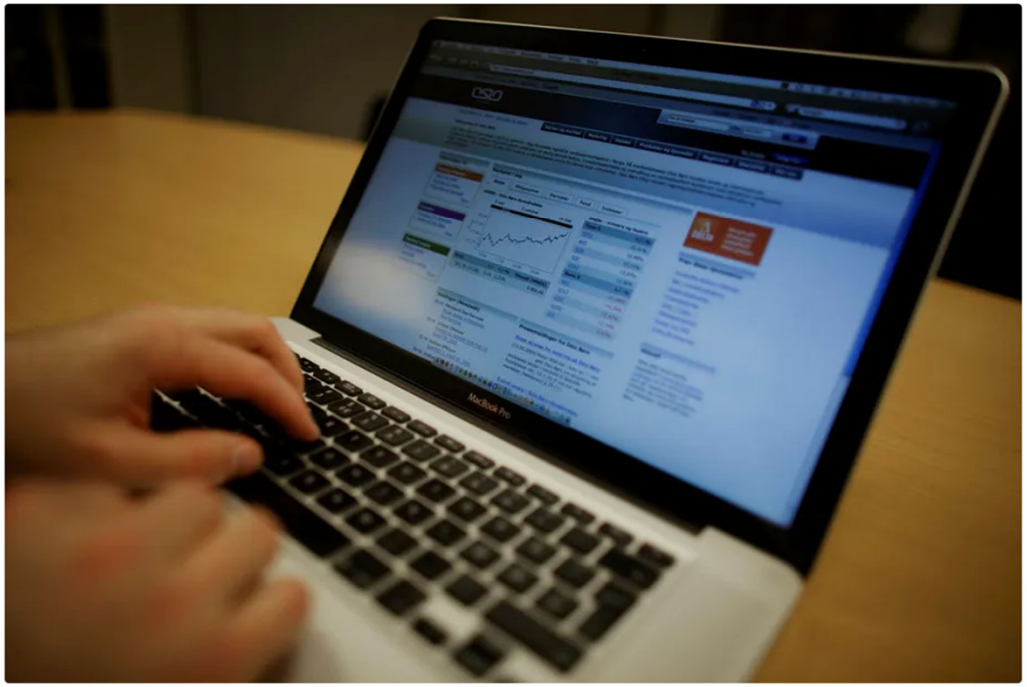
Politioverbetjent, Kripos

KiNS Tech 2024 | 26.09.2024

POLITIET
KRIPOS

Energiselskap i Rogaland svindlet for 150 millioner kroner

Et energiselskap i Stavanger-regionen ble i høst svindlet for 150 millioner kroner gjennom et såkalt direktørbedrageri, skriver Stavanger Aftenblad.



(Dn.no 28.11.19)

POLITIET
KRIPOS

NC3, Kripos

- **N**ational **C**yber**c**rime **C**entre (Nasjonalt Cyberkrimsenter)
- Opprettet i 2019
- 160 ansatte
- Etterforskning, etterretning og forebygging
- Bistandsorgan for politidistriktene
- Metodeutvikling og grenseoverskridende kriminalitet

POLITIET
KRIPOS

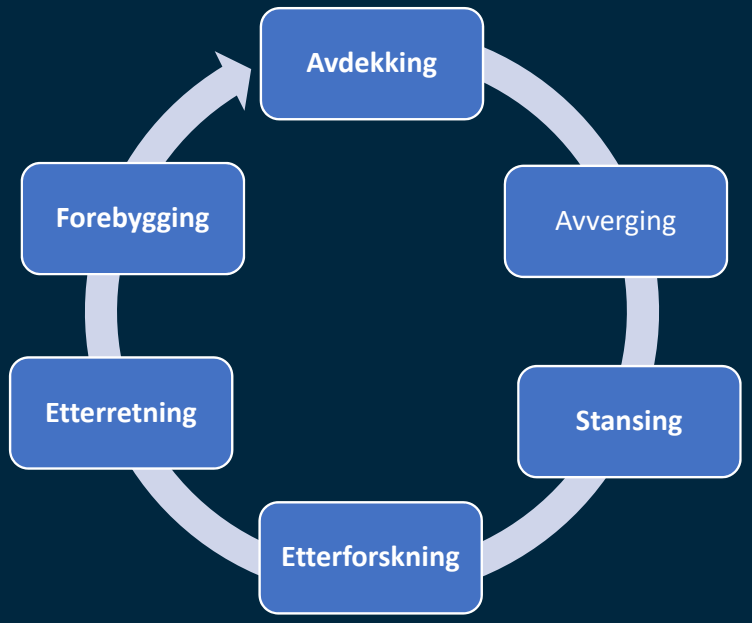
Agenda

- Politiets rolle
- Anmeldelsen
- Den fysiske og digitale sfære
- Etterforskningen
- Andre polisiære formål
- Anbefalinger

POLITIET
KRIPOS

Politiets rolle

- Etterforskning = tvangsmidler
- Søker å besvare hvem, hva, hvor, hvorfor, hvordan og når



POLITIET
KRIPOS

Anmeldelsen

- Anmeld!
- Store mørketall
- Ulike anmeldelsesformer
- Pilot for digital løsning i 2025

Overordnet kategori	Anmeldelsesform	Antall saker
Digital	Digitalt skjema	4
	E-post	12
Papirformat	Håndskrevet skjema	7
	Brev	3
Avhør	Avhør – oppmøte politi	5
	Avhør – hos fornærmede	1
	Totalt:	*32*

POLITIET
KRIPOS

Den fysiske og digitale sfære

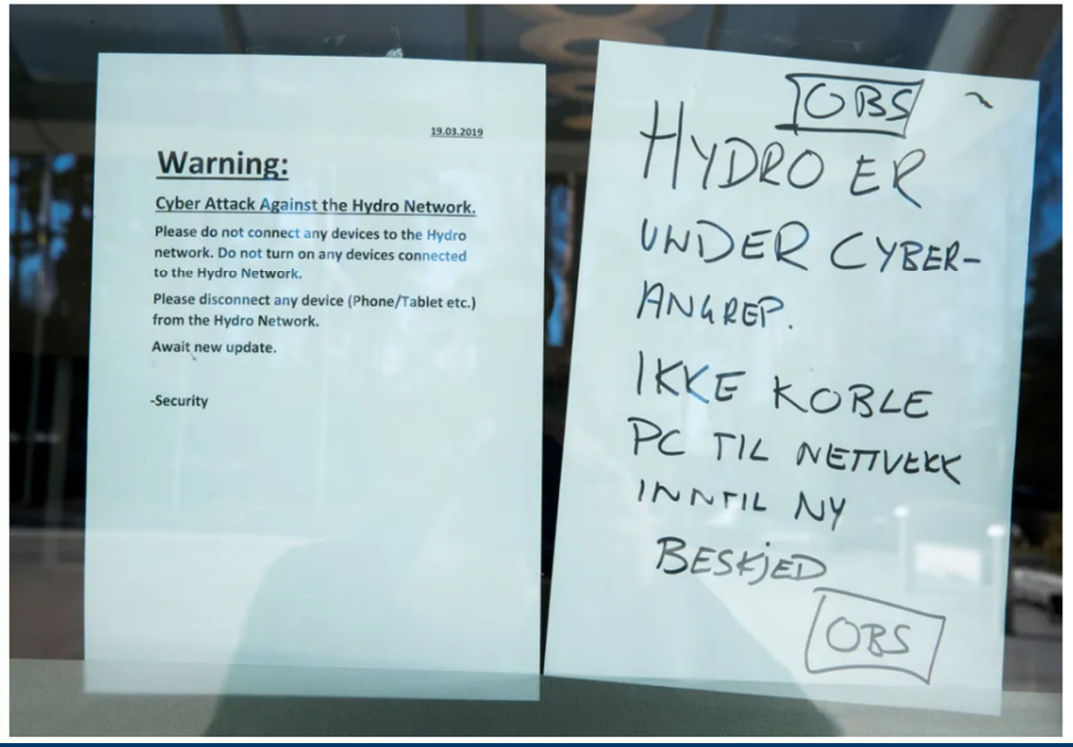
- Straffeloven er teknologinøytral
- Enhetlig begrepsbruk

POLITIET
KRIPOS

POLITIET
KRIPOS

Hydro rammet av hackerangrep

IT-systemer i de fleste forretningsområdene er påvirket. Selskapet sier de skifter til manuell drift så langt det er mulig.



(Digi.no, 19.03.19)

POLITIET
KRIPOS

Hva bør anmeldelsen inneholde?

- Rett myndighet / fullmakt til å anmelde
- Beskrivelse av hva som har hendt
- Verdivurdering av det som er stjålet/ødelagt
- Kontaktpersoner
- Samtykke til å dele informasjon med politiet
- Dokumentasjon

POLITIET
KRIPOS

Hva slags data trenger vi?

- Virksomhetens eksterne IP-adresse(r)
- Inngangsvektor
- Mistenkelige IP-adresser med tidsstempel (tt:mm:ss) og tidssone (UTC)
- Mistenkelige domener
- Kommunikasjonsprofiler
- Betalingsadresser og transaksjonsopplysninger
- Kopi av løsepengebrevet, mailer, telefonlogg ol.
- Informasjon om skadevare

POLITIET
KRIPOS

Hvordan ønsker vi å motta data?

- Kopi av hendelsesrapporter og avviksskjema
- Excel, tekst-format, csv ol.
- Søkbart!

POLITIET
KRIPOS

Utfordringer

- Samarbeide på tvers av sektorer

POLITIET
KRIPOS

Minst 400 nordmenn er blitt lurt til å oppgi BankID til svindlere i Romania. Det samlede tapet er sannsynligvis på mange millioner kroner.

Gjerningspersonene i sakskomplekset har sendt ut over 10.000 målrettede SMS-er som fremstår som de kommer fra Statens vegvesen. Økokrim tror det er store mørketall i saken, som i saker der fornærmede ikke har anmeldt fordi banken har dekket tapet.

Økokrim har også samarbeidet med private aktører, som blant annet BankID og Visma under etterforskningen av saken så langt.

– De private aktørene har bidratt til at politiet har kunnet identifisere personer som vi mener står bak de digitale bedrageriene i Norge. Det har vært et viktig bidrag inn i etterforskningen, og vi ønsker å takke dem for et godt samarbeid sier Allum.

Økokrim har også fått bistand fra rumenske DIICOT (Directorate for Investigating Organized Crime and Terrorism) og det nasjonale politiet (Romanian National Police – Combatting Organized Crime Directorate, Cybercrime Unit). (©NTB)

(tu.no, oktober 2023)

POLITIET
KRIPOS

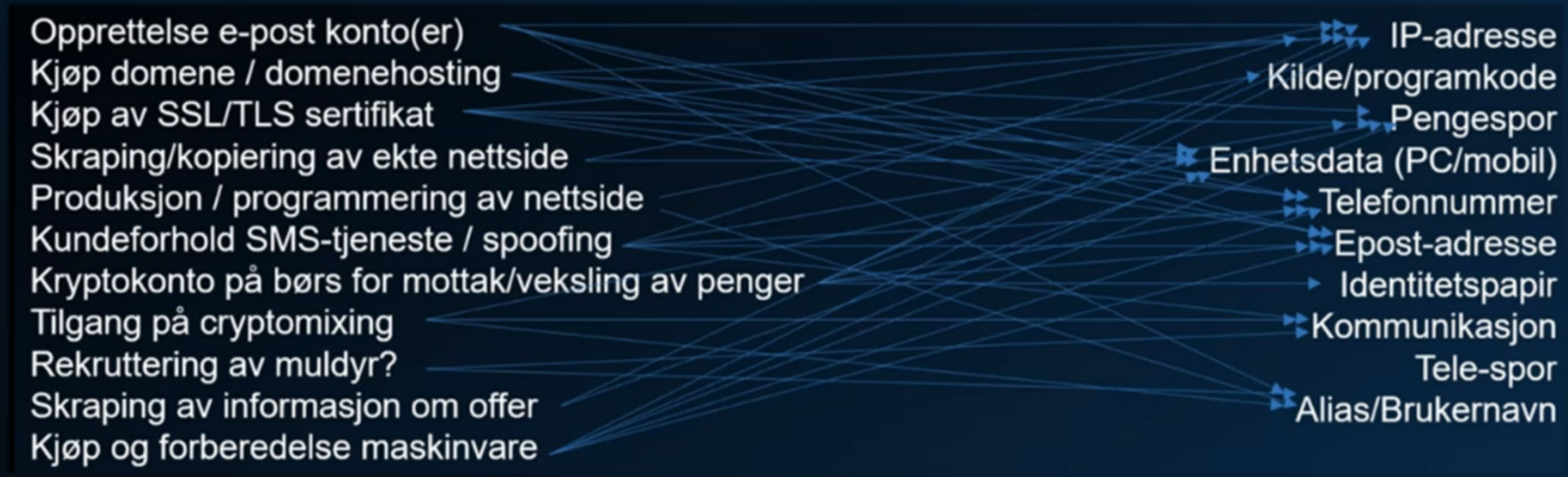
Utfordringer

- Samarbeid på tvers av sektorer
- Internasjonalt samarbeid
- Sporstedene

POLITIET
KRIPOS

SPORKILDER

MULIGE SPORTYPER



POLITIET
KRIPOS

Utfordringer

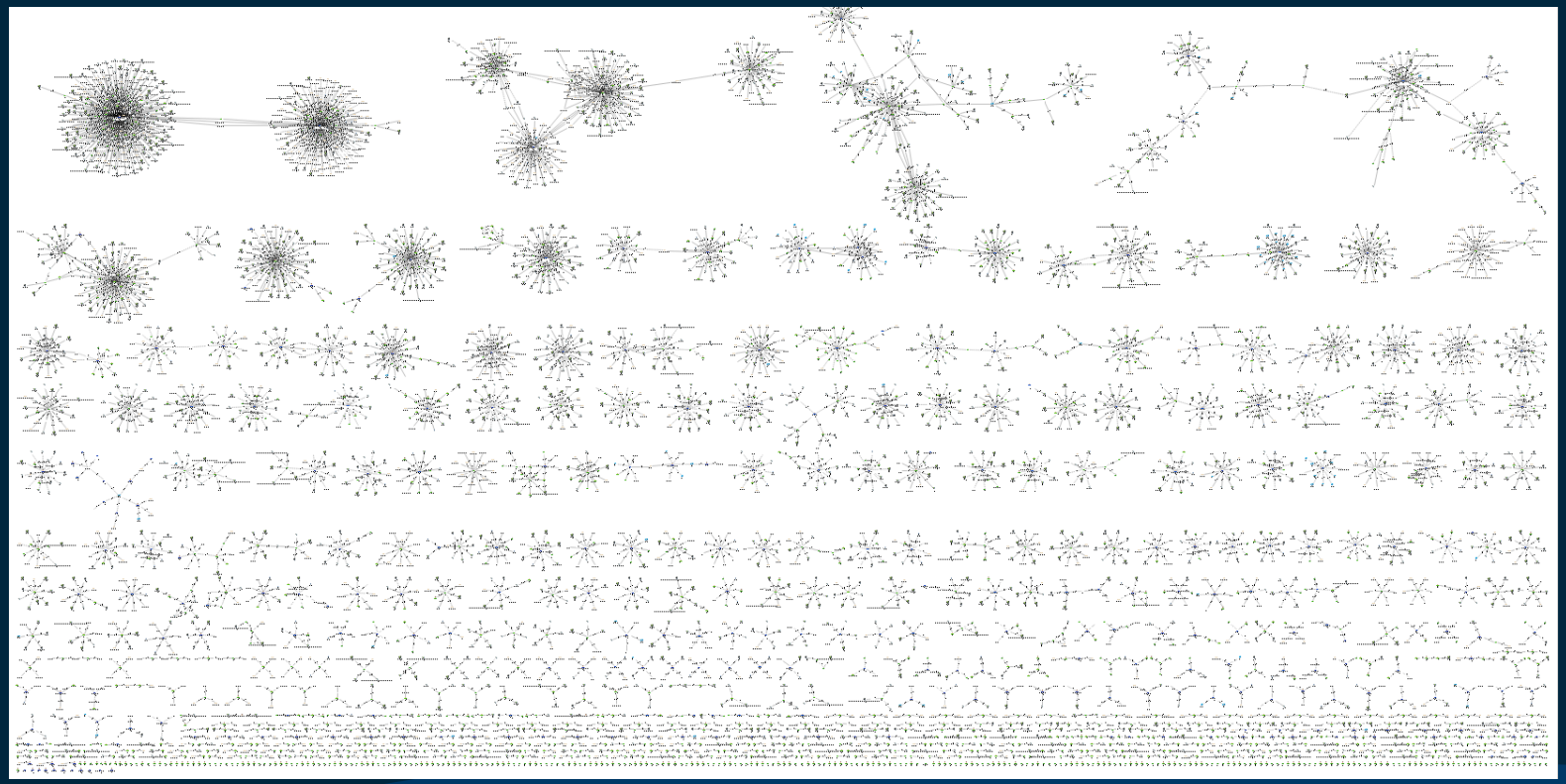
- Samarbeid på tvers av sektorer
- Internasjonalt samarbeid
- Sporstedene
- Datamengden
- Ny teknologi krever nye metoder
- Politiets modenhet

Politiet har stått bak åtte datainnbrudd. Ny, omstridt politimetode brukes stadig oftere.

Norsk politi har gjennomført åtte datainnbrudd etter at en ny lov åpnet for at politiet kan bruke de samme metodene som hackere og datasvindlere.

(Aftenposten, 18.10.2019)

POLITIET
KRIPOS



KiNS Tech 2024 | 26.09.2024

POLITIET
KRIPOS

POLITIET
KRIPOS

Flere pågrepet etter Hydro-angrepet

I det krigsherjede landet har ukrainsk cyberpoliti sparket inn dører over hele Kyiv på jakt etter hackere. Identitetene deres stammer fra en fem år lang norskledet politietterforskning.

(vg.no, 28.11.23)

POLITIET
KRIPOS

KiNS Tech 2024 | 26.09.2024

POLITIET
KRIPOS

17. juni 2024, 16:33 **Redaksjonen**

Har du en Asus-ruter, bør du oppdatere fastvaren nå

Selv om det uansett er viktig å installere fastvareoppdateringer til bredbåndsrutere med jevne mellomrom, er det ekstra viktig for eierne av utvalgte Asus-rutere å gjøre dette akkurat nå. Asus har kommet med en sikkerhetsoppdatering som fjerner en svært alvorlig sårbarhet i sju ulike modeller, inkludert den eldre, men mye solgte RT-AC68U-modellen.

Sårbarheten gjør det mulig for angripere å omgå autentiseringen, slik at de kan ta kontroll over ruteren via internett. Dette skriver Bleeping Computer.

Oppdateringen kan enklest installeres ved hjelp av det innebygde, webbaserte oppdateringsverktøyet. Dersom man ikke har mulighet til å installere oppdateringen raskt, bør tjenester eksponert mot internett, inkludert videresending av porter, DDNS, VPS-server og demilitarisert sone (DMZ), deaktiveres.

(digi.no)

POLITIET
KRIPOS

Anbefalinger

- Fjerne gamle maskiner / brukere
- Oppdater programvare
- Bytt standardpassord
- Passordbeskytt / krypter sensitive data
- Aktiver to- eller multifaktorautentifisering
- Isoler backup'en
- Aktiver tilstrekkelig logging
- Monitorering
- Lag gode interne rutiner

POLITIET
KRIPOS

– Konsekvensene ble mindre enn de kunne blitt

(22.02.22) – Nortura var utsatt for et alvorlig dataangrep, men vi var godt forberedt og avverget kryptering av systemene våre. Vi har en godt drillet beredskapsorganisasjon, gode planer og vi hadde øvd på liknende scenarioer kort tid før angrepet. Det førte til at konsekvensene ble mindre enn de kunne ha blitt. Nå jobber vi på spreng for å få på plass nye permanente dataløsninger, og sikre oss enda bedre, sier konsernsjef Anne Marit Panengstuen.

(nortura.no, 22.02.22

POLITIET
KRIPOS

Spørsmål?

POLITIET
KRIPOS

Takk for meg!

KiNS Tech 2024 | 26.09.2024