POLITIET

Norwegian Police

Informasjon fra Oslo politidistrikt

Fra: Næringslivskontakt/politiinspektør Christina T. Rooth Oslo politidistrikt
Seksjon for Digitalt politiarbeid og innovasjon Oslo politidistrikt

Dato: 24.5.22

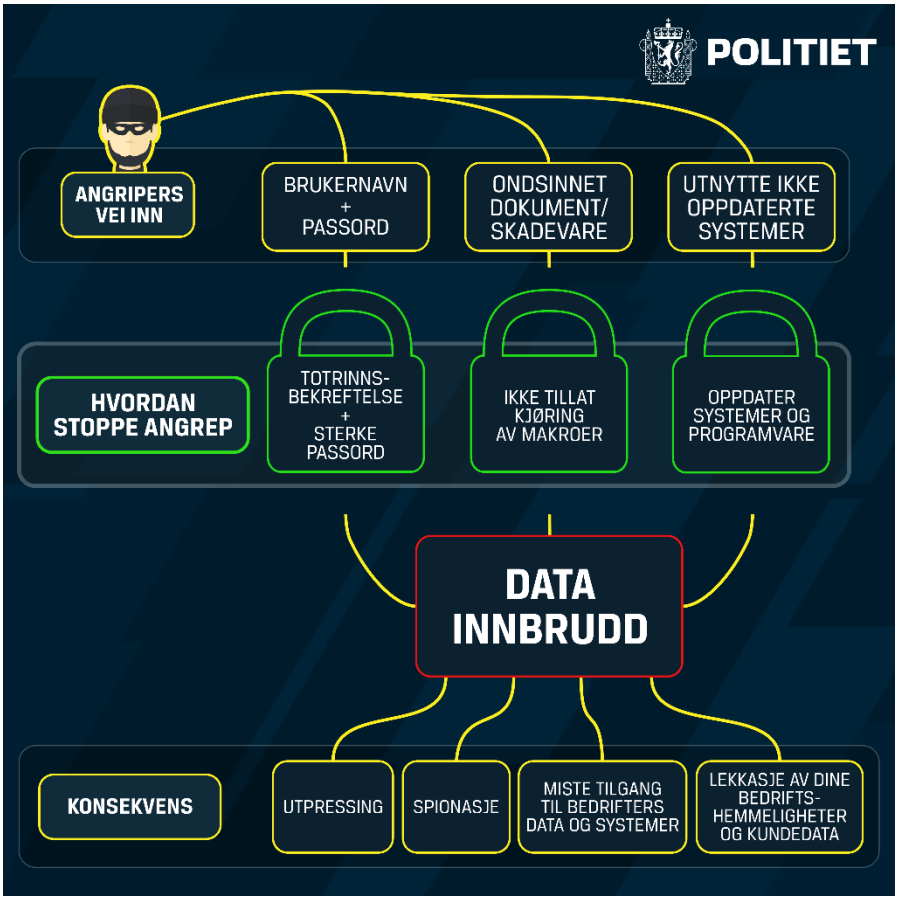
Beskytt bedriften din mot datainnbrudd & digital utpressing

Datainnbrudd og løsepengevirus er kriminalitetsfenomener som vil kunne berøre ALLE norske offentlige og private virksomheter i årene som kommer, se politiets trusselvurdering 2022, pkt 5. Politiets trusselvurdering 2022.

Et slikt angrep kan ha store konsekvenser for din virksomhet og vi har eksempler på virksomheter som har gått konkurs som følge av dette.

Selv om trusselbildet har blitt skjerpet, betyr ikke dette nødvendigvis betydelig økt risiko. Sårbarhetene kan reduseres og risikoen kan holdes på et akseptabelt nivå ved at man sørger for en tilstrekkelig grunnsikring.

Oslo politidistrikt etterforsker flere saker som dreier seg om digital utpressing. På bakgrunn av det vi ser i disse sakene, ønsker vi å gi informasjon om noen få tiltak som vi mener er spesielt viktig å iverksette, og som vil redusere risikoen betraktelig. Disse tiltakene mener vi det burde være mulig å gjennomføre uansett størrelse, og uansett hvilken IKT- kompetanse som er i din virksomhet.



Bilde: Angripers vei inn, og hvordan du kan forebygge dette

OSLO POLITIDISTRIKT
Post: Postboks 2093 Vika, 0125 Oslo / (+47) 22 66 90 50
post.oslo@politiet.no / www.politiet.no / 961 398 142

Dette er tiltak som bør iverksettes!

- Benytt totrinns bekreftelse og sørg for at alle brukere har sterke unike passord.

- Blokker kjøring av makroer i Office filer. Dette høres kanskje ukjent ut, men det er viktig for å hindre at angriper får tilgang til dine systemer. Les her, "Endre makroinnstillinger i klareringssenteret": https://support.microsoft.com/nb-no/office/makroer-i-office-filer-12b036fd-d140-4e74-b45e-16fed1a7e5c6

- Sørg for å holde maskiner og programmer oppdatert og installer sikkerhetsoppdateringer så raskt som mulig. Slå av eller koble fra maskiner som ikke er i bruk.

- Fjern brukere og tilganger dere har som ikke er nødvendige.
  Administratorrettigheter må begrenses. De som har kontoer med administratorrettigheter anbefales på det sterkeste å ha en annen brukerkonto som kan benyttes mot internett og i daglig drift.

- Ta sikkerhetskopi av data bedriften er avhengig av for å kunne fungere. Slik at du har noe å gjenopprette ifra om du skulle bli utsatt for et angrep og alt skulle bli kryptert eller slettet.

Nød plakat: Hvis din virksomhet blir utsatt for digital utpressing så har Næringslivet Sikkerhetsråd laget en nød plakat med viktige kontaktpunkter. Denne kan være hensiktsmessig å ha fysisk tilgjengelig ved behov.

Den lille brosjyren om datasikkerhet: Oslo politidistrikt har sammen med Kripos (NC3) også laget en liten brosjyre med forebyggende råd når det gjelder bedragerier og datakriminalitet som det også anbefales å lese. Den lille brosjyren om datasikkerhet.

NSM: For ytterligere tiltak og informasjon så se NSM sine sider: Digital beredskap i en skjerpet situasjon - Nasjonal sikkerhetsmyndighet (nsm.no)