HUNN/GJØVIK ROTARYKLUBB.

08.12.2020

REFERAT FRA MEDLEMSMØTE 8. DESEMBER 2020

Møtet ble avviklet som Teamsmøte på grunn av smittefaren fra covid – 19.
21 medlemmer deltok fordelt på 20 maskiner.
Heidi Videhi Røsdal holdt foredrag om «IT-sikkerhet i hverdagen».

President Torbjørn Skogsrød ledet møtet.
Treminuttersinnlegget var ved Ottar Lied. Han snakket om skam-begrepet og ordsammensetningene med skam, som har dukket opp i den senere tid, fly-skam. kjøtt-skam etc.

Heidi Videhi Røsdal har bakgrunn som sikkerhetsansvarlig i Aquatic Chemistry, Lillehammer, og er derfor daglig konfrontert med datasikkerhet i et stort konsern. Hun poengterer at IT er et fantastisk redskap for informasjonsdeling og rasjonalisering av arbeid, samtidig som det gir folk som ikke vil oss vel store muligheter. Dette er både enkeltpersoner, organiserte grupper og stater. De vil stjele penger eller informasjon, de vil sabotere eller desinformere (jfr. fake news).
Store firmaer, som etter hvert har fått gode sikkerhetssystemer, opplever kontinuerlig massive angrep, som noen ganger lykkes, men en akilleshæl er enkeltpersonene som jobber der. Også privat utsettes vi for IT-svindel.
Foruten økende IT-kompetanse har angriperne lært seg å utnytte angst, stress, tidspress, nysgjerrighet hos medarbeiderne.
Angrep kan skje via e-post, en nettside, sosiale medier eller SMS-meldinger som inneholder en skadelig lenke. Det kan også skje via et gratis usikret nettverk, f.eks. på CC eller Gardermoen, eller via en oppringning.
Gjennom en skadelig lenke kan noen infisere et større nettverk og tappe det for informasjon eller skade det. Og de kan blokkere maskiner eller nettverk og kreve løsepenger (Ransomware).
Phishing vil si at man er ute etter personopplysninger som kan brukes til identitetstyveri, eller firmaopplysninger.
Såkalt direktørsvindel kan bestå i at man får melding om å overføre et større beløp til en konto, og at dette haster veldig. Det skjer gjerne på et tidspunkt med mye stress.
Masseutsendelse fra posten eller banken om en pakke på vei, eller at ett eller annet må oppdateres, er gjerne lett å gjennomskue, men statistisk sett er det alltid noen som går på limpinnen, særlig om man faktisk venter en pakke i posten.
Kryptokapring vil si at noen tar kontroll over maskinen for å stjele datakraft. Om maskinen plutselig blir veldig treg, kan dette være årsaken.

For å møte trusselen er årvåkenhet og oppdatert programvare med beskyttelsesprogram det grunnleggende. Er du tvilende til en adresse, så hold musepekeren over den, men uten å klikke. Stoler du ikke på en lenke, så gjør det samme for å undersøke nøyere hvem som kan være avsender. Ikke koble deg på usikrede åpne nettverk. Studer språk og layout, som er blitt mer profesjonelt enn før, men hvis ordforråd og uttrykksmåte i en for øvrig korrekt tekst avviker fra den oppgitte avsenderens språkbruk, er det fare på ferde.

Nettet er en effektiv spreder av konspirasjonsteorier, løse rykter og løgn. Det er alles ansvar ikke å delta i å spre den slags. Spør deg: Er dette sannsynlig? Hva er konteksten? Hvem er kilden? Kan andre kilder bekrefte det? Når ble dette sendt? Er det ment som en spøk/satire?

Foredraget ble etterfulgt av flere spørsmål og kommentarer. Det ble spurt om hvordan enkeltmannsforetak og små firmaer uten store ressurser kan beskytte seg. Svaret var å kjøpe en datahjelp, gjerne gjennom en forhandler.

Vi hadde premiere på datastøttet vinlotteri, gjennomført med stødig hånd av Arne Erik Haldsrud. Den heldige vinner denne gangen var Bjørn Øversjøen. Men det kommer stadig nye sjanser.

Ref: Ola Rongen