Digitale trusler og informasjonssikkerhet

Næringsliv og offentlig forvaltning preges nå av økende digitalisering. Det fører til at virksomhetene blir mer effektive og lønnsomme, men også til en økende fare for at virksomheter kan settes ut av spill eller lide betydelige tap.

Det er mange eksempler på at bedrifter har gått under etter digitale angrep. I 2016 økte f.eks. antallet angrep av løsepengevirus mot bedrifter i USA med hele 6 000 %. Også norske virksomheter er i økende grad utsatt for digitale angrep. Eksportindustrien er særlig utsatt - spesielt teknologibedriftene.

Digital industrispionasje er ofte billigere og langt mer effektiv enn tradisjonelle metoder. Det drives derfor utstrakt grad av slik aktivitet rettet mot norske virksomheter. Både offentlige og private aktører står bak. Angrepene er ofte sofistikerte og målrettede.

Her er våre råd for beskyttelse mot digitale trusler:

Nettsider
Falske nettsider er ofte brukt til å infiltrere PCer og derfra virksomhetens IT systemer. Ofte ser sidene originale ut, men kan avsløres f.eks. på at navnet ligner på original siden. Ikke last ned fra sider du ikke er helt sikre på. Se etter tegn på autentisitet. Gi aldri fra deg opplysninger om identitet, personopplysninger, passord e.l. på nettsider. Om du blir bedt om kredittkortopplysninger er det ekstra viktig å sjekke autentisiteten.

E-post
E-post er den enkleste og derfor mest brukte mulige inngangsport til virksomhetens IT systemer og derfor til å stjele konfidensiell informasjon eller skade bedriften. Skadevaren opptrer gjerne som lenker i eller vedlegg til e-posten. Åpne derfor ikke lenker eller vedlegg uten at du er 100% sikker på avsenderen. Bruk aldri private e-post kontoer til informasjon som gjelder virksomheten. Bruk uansett aldri e-post til å sende konfidensiell informasjon ukryptert.

SMS
Bruk aldri SMS til konfidensiell informasjon. Om du absolutt må sende en konfidensiell tekstmelding, bruk da heller krypterte tjenester som Signal, WhatsApp eller Messenger. NB! Sikkerhetsgradert informasjon skal alltid bare formidles på de måter sikkerhetsmyndighetene (NSM) tillater.

Mobiltelefon
Det verdensomspennende mobiltelefonnettet er lett å bryte inn i. Det samme gjelder telefonene vi bruker, uansett merke. Med kommersielt tilgjengelig teknologi er det enkelt å avlytte samtaler, skaffe tilgang til e-post og SMS o.a. lagret på telefonene, samt å overvåke brukeren vha. telefonens mikrofon og kamera. Mobiltelefonen bør derfor

aldri brukes til å formidle eller lagre konfidensiell informasjon. Uansett bør alltid mobiltelefonen være utstyrt med adgangspassord og mulighet for fjernsletting av alt innhold. I en del land er risikoen for å få telefonen forurenset så stor at den bør destrueres etter bruk. Om det er helt nødvendig å bruke mobiltelefon til konfidensiell informasjon, bør man anskaffe telefon med krypteringsteknologi.

Romavlytting
Avlytting av møterom og andre lokaler er enkelt og billig med teknologi som er lett tilgjengelig på nettet. Det kan være en god ting å ha i alle fall ett møterom som regelmessig blir sjekket for avlyttingsutstyr og er kontinuerlig beskyttet.

Bærbare PCer og nettbrett
Bærbare maskiner er ofte på reise og derfor lett å stjele. Sørg for å ha et sikkert adgangspassord og aldri lagre konfidensiell informasjon på maskinens harddisk. Koples maskinen til fremmede nettverk er det stor risiko i enkelte land for at den blir infisert med programvare som kan trenge inn i bedriftens IT systemer når maskinen koples opp til hjemmenettverket. Som med mobiltelefoner er det etter besøk i slike land tryggest å destruere PC og nettbrett etter bruk.

Skytjenester
Mange virksomheter bruker skytjenester til lagring og utveksling av informasjon. Det er en god regel ikke å tillate bruk av andre skytjenestekonti enn den eller de virksomheten har opprettet. Opprett konti for virksomheten bare på tjenester du er sikker på.

NSMs fem råd om IKT sikkerhet
Norske virksomheter utsettes daglig for digitale angrep. Etter Nasjonal Sikkerhetsmyndighets (NSM) erfaring vil flg. fire tiltak stoppe 80 – 90 % av alle dataangrep:

1. Oppgrader program- og maskinvare løpende.
2. Installer sikkerhetsoppdateringer
3. Ikke tildel administrator-rettigheter til sluttbruker.
4. Blokker kjøring av ikke-autoriserte programmer

Holdninger og bevissthet
Det viktigste tiltaket er å skape holdninger til sikkerhet og bevissthet om truslene gjennom kunnskap og tydelige retningslinjer fra bedriftens ledelse. Like viktig er det at ledelsen selv praktiserer og følger opp bedriftens policy – «the tone from the top».

Søk råd
Multisys hjelper private og offentlige virksomheter med tiltak mot digitale angrep. En god begynnelse er å skaffe oversikt over virksomhetens informasjonsverdier, hva som kan true og hvor sårbar verdiene er for angrep. Her som ellers er det svakeste ledd som regel avgjørende for sikkerheten. Det er da ofte en fordel at noen utenfra tilfører virksomheten kunnskap om og innsikt i egne sikkerhetshull. Multisys kan utarbeide en statusrapport for din virksomhet, samt gi råd om forebyggende tiltak.