Trusler i vår digitale hverdag – mot individer og virksomheter

Trusler og trender 2017–18

NorSIS
Norsk senter for informasjonssikring

Innhold

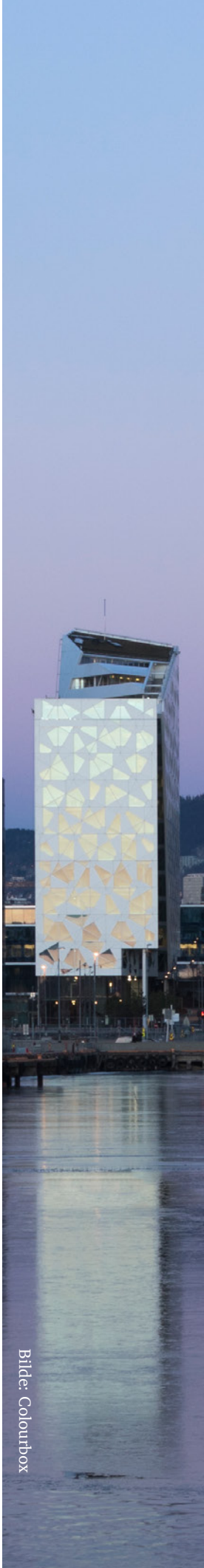
Trusler og trender er en årlig rapport utgitt av Norsk senter for informasjonssikring (NorSIS). Rapporten avtegner status for norsk informasjonssikkerhet på utgivelsestidspunktet, vurderer de alvorligste truslene norske privatpersoner og virksomheter står overfor i det digitale rom, og skisserer de mest framtredende trendene innenfor datakriminalitet.

Trusler og trender ser trusselbildet primært ut fra sårbarheten til enkeltindividet og familien i privatsfæren, og små og mellomstore selskaper i virksomhetssfæren. Til den siste kategorien hører også offentlige virksomheter, inklusive kommuner. Dette perspektivet sammenfaller med målgruppeorienteringen til NorSIS, og supplerer offentlige norske risiko- og trusselrapporter.

Trusler og trender skal ses i sammenheng med råd om tiltak som fortløpende oppdateres på våre tjenester Slettmeg.no og Nettvett.no.

STATUS

2017



Bilde: Colourbox

Utvikling av samfunnet

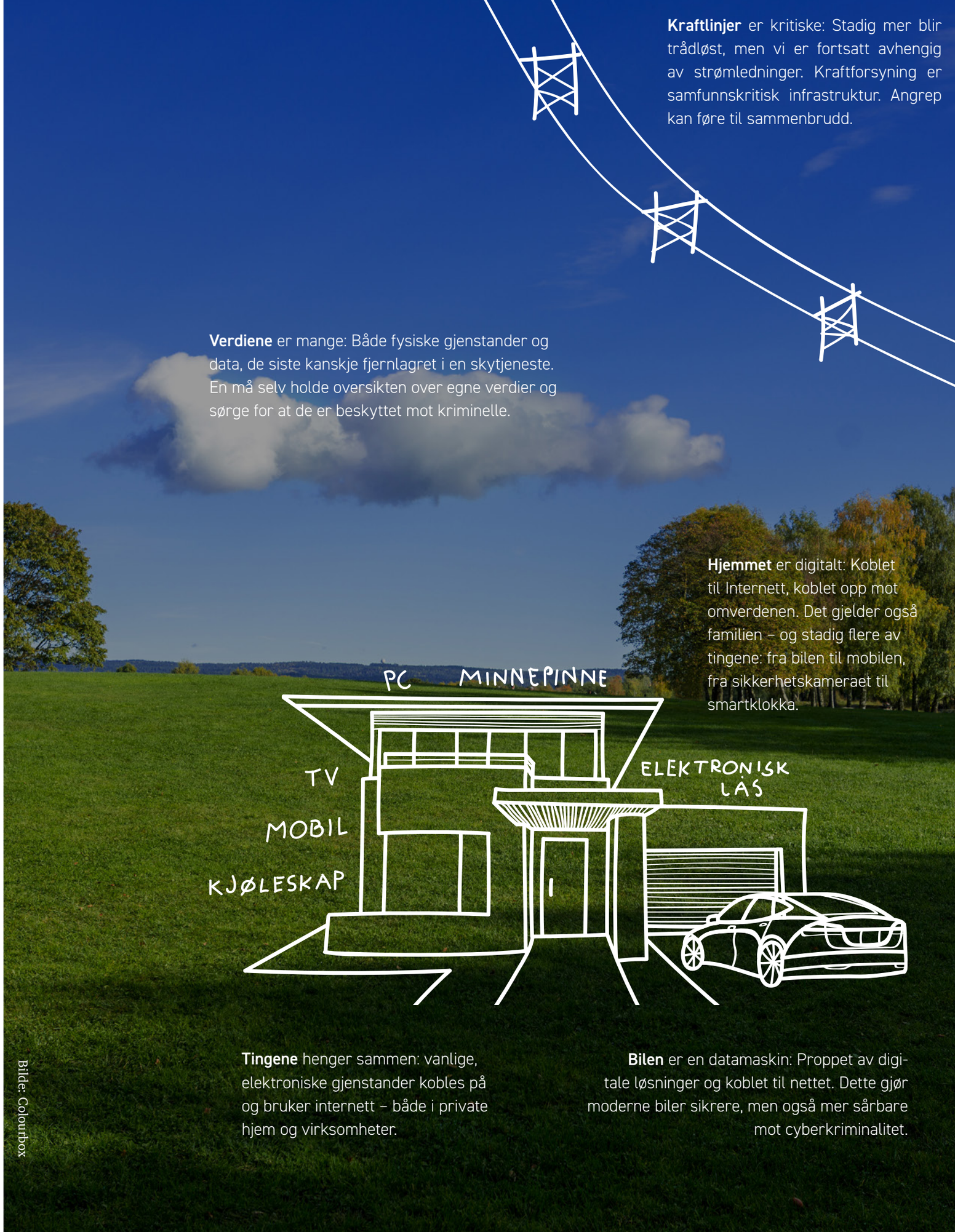
Den digitale hverdagen

Hverdagen er digital. Enten vi legger merke til det eller ikke blir en stadig større del av livet vårt påvirket av digitalisering. Dette er et gode, når utviklingen og løsningene gjør hverdagen lettere. Det forutsetter at mulighetene som skapes ikke medfører mer enn akseptabel risiko. Digitalisering medfører trusler – som må tas hensyn til og ivaretas med tiltak. Målet vårt er en trygg digital hverdag – for alle.

Digitalisering endrer hjemmene våre, og hvordan vi lever våre liv. Flere ting i hjemmet er digitale – og koblet til internett. I hjem og på fritid utnyttes digitale løsninger til fornøyelse og nytte, også for bedre sikkerhet. Hjemmet kan bli sikrere med en nett-tilkoblet brannvarsler og trygghetsalarm. Dét kan samtidig skape nye digitale sårbarheter, som igjen kan utnyttes av cyberkriminelle.

Organisert kriminalitet har flyttet seg mer over i det digitale rom. Dette er en global utfordring, og de kriminelle slår til der det er verdier å hente – og sårbarheter å utnytte. De færreste, verken på hjemmebane eller i virksomheter, vet egentlig hva de risikerer å miste: hvilke verdier de faktisk har, materielle og immaterielle, og hvor utsatt de er for angrep – og tap.

Målrettet cyberkriminalitet retter seg både mot privatpersoner og virksomheter, og i tiltagende grad de sistnevnte, der verdiene er størst. Små og mellomstore bedrifter er lettest å ramme. Sårbarhetene øker i takt med digitaliseringen av samfunnet, som fører til et arbeidsliv i endring. Skillet mellom hjem og arbeidsplass viskes for mange gradvis ut.



Kraftlinjer er kritiske: Stadig mer blir trådløst, men vi er fortsatt avhengig av strømledninger. Kraftforsyning er samfunnskritisk infrastruktur. Angrep kan føre til sammenbrudd.

Verdiene er mange: Både fysiske gjenstander og data, de siste kanskje fjernlagret i en skytjeneste. En må selv holde oversikten over egne verdier og sørge for at de er beskyttet mot kriminelle.

Hjemmet er digitalt: Koblet til Internett, koblet opp mot omverdenen. Det gjelder også familien – og stadig flere av tingene: fra bilen til mobilen, fra sikkerhetskameraet til smartklokka.

Tingene henger sammen: vanlige, elektroniske gjenstander kobles på og bruker internett – både i private hjem og virksomheter.

Bilen er en datamaskin: Proppet av digitale løsninger og koblet til nettet. Dette gjør moderne biler sikrere, men også mer sårbare mot cyberkriminalitet.

Bilde: Colourbox

Skyen er svevende: Der lagres enorme datamengder, ikke i en vanlig sky, men på servere – ett eller annet sted, driftet av noen. Sikkerheten er stor, men kundene bør vite hva de har betrodd til hvem og hvor.

Rådhuset skal levere: Offentlig sektor, statlig og kommunal, skal digitalisere seg selv og de tjenester de leverer til samfunnet. Framtidig velferd, trygghet og trivsel avhenger av det.

Veien er viktig: Fysiske samferdselsårer – på land, i lufta og på havet – er like viktig nå som før. De blir også digitaliserte. Sensorer i veibanen kommuniserer med biler, og med sikringsmekanismer.

Fiber

Nettet er nødvendig: Fysiske nett – kabler og koblingspunkter – er grunnmuren for internett. Det er på mange måter blitt den viktigste, og mest samfunnskritiske, kommunikasjonskanalen.

Skolen er sentral: Her går storbrukere av digitale tjenester, her formes holdninger og fremmes nettvett. Her er unge databrukere som ofte er under betydelig press – også på internett.

Tjenesteutsetting er utbredt: Digitale tjenester, inkl. drift, kjøpes, også gjennom utsetting til eksterne aktører. Outsourcing utfordrer (og bedrer) sikkerheten, herunder kontroll med sensitiv personinformasjon.

Selskaper skal leve: Privat sektor, store og små selskaper, skal konkurrere innen sektorer og på markeder i rivende utvikling. Framtidig verdiskaping krever digitalisering og innovasjon.

Bilde: Colourbox

Det digitaliserte samfunnet

Samfunnet er digitalisert. Enten vi vil det eller ei blir stadig flere samfunnsfunksjoner digitale. Dette gir oss muligheter, som skaper mer innovasjon, økt effektivitet og bedre velferd. Mennesket må da settes i sentrum, med digitalisering som et middel, ikke som et mål i seg selv.

Digitalisering endrer samfunnet vårt, og hvordan virksomheter utvikles og drives. Offentlig sektor gjennomgår en offensiv modernisering med å effektivisere prosesser og tilgjengeliggjøre tjenester overfor innbyggerne. Virksomheter er avhengig av digitale løsninger, og blir mer og mer integrert i leverandørkjeder, ofte på tvers av landegrenser. Verdikjedene blir lange og komplekse. Dét åpner også for sårbarheter, som utnyttes til cyberkriminalitet

Overblikk over situasjonen

Birgit ble svindlet for 1,3 millioner

in historie for å advare andre. Foto:

14. juni 2017, kl. 18:39

Morten deler identitet med en kriminell

Kun en tredjedel anmelder ID-tyveri. Manglende tillit til politiet kan være årsaken, viser undersøkelser. Morten Arntun opplevde at en fremmed brukte kortet hans til å kjøpe flybilletter og varer for 22.000 kroner. Politiet henla saken.

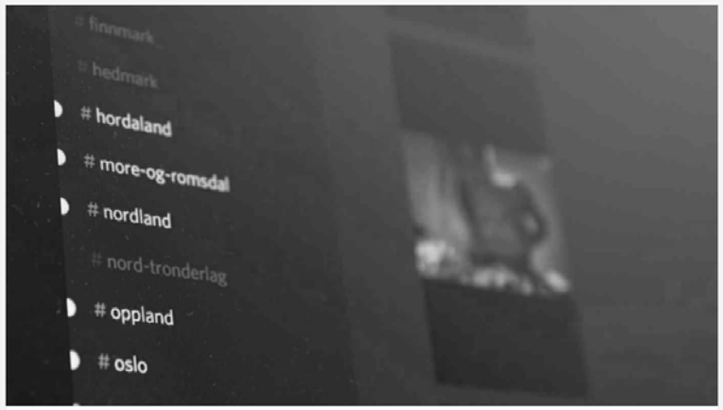
Amanda Rørmark Åsberg
Journalist

Publisert 20.03.2017, kl. 05:26

Morten Arntun ble utsatt for identitetstyveri og svindel.
FOTO: AMANDA ÅSBERG / NRK

FORUM PÅ HEMMELIG APP SPRER SEG OVER HELE LANDET:

Nakenbilder av hundrevis av norske jenter deles på det mørke nettet



FORDELT PÅ FYLKER: Bildene inne på appen er fordelt på fylker. Medlemmene kan også komme med navn på jenter de ønsker bilder av. Foto: Simen Askjer / TV 2

Petter Stordalens Choice Hotels er blant virksomhetene som er rammet av det internasjonale dataangrepet.
Foto: Terje Pedersen/NTB Scanpix

Nyheter Teknologi

Choice Hotels ble rammet av WannaCry

TUNG TID: Nora Mørk fikk hverdagen snudd på hodet da én person hacket mobiltelefonen hennes og spredde private bilder nettet. Foto Dagbladet

Private bilder av Nora Mørk på avveie

Utga seg for å være direktør: Svindlet festspillene i Nord-Norge for 770.000 kroner

2.400 euro, cirka 770.000 norske kr

Fikk du denne e-posten fra Skatteetaten i dag? Ikke trykk på lenka

Ble du glad da du så eposten fra Skatteetaten der det stod «Vi har funnet ut at du er berettiget til å motta en skatterefusjon 3.950 NOK»? Den er ikke ekte.

Svar Svar til alle Videresend Direktemelding

on 12.07.2017 15:43

Skatteetaten < . @ska

Ny melding

Til NRK Rogaland

Kjære kunde,

Vi har funnet ut at du er berettiget til å motta en skatterefusjon 3.950 NOK.
Klikk her for å motta din skatt tilbakebetaling.

Syed Ali Shahbaz Akhtar
Journalist

Oppdatert 12.07.2017, kl. 21:01

NRK har fjernet navnet på avsender. Denne eposten ble sendt til en fellesadresse.
FOTO: SKJERMDUMP / NRK

Nyheter

Også norske bedrifter mål:

– Alvorlige dataangrep fra Kina

Ole Peder Gjæver
5. april 2017 15:40 – Oppdatert 6. april 2017 09:28

Del (62) Tweet Epost

Norge, Sverige og Finland er blant landene den kinesiske hackerligaen APT10 skal ha rammet. Faksimile fra rapporten «Operation Cloud Hopper», den offentlige delen av undersøkelsene til PwC UK, BAE Systems og britiske National Cyber Security Centre.

Sikkerhetstjenesten: Avslørte spionasje-angrep mot norske forskere

HACKET: Kommunikasjonssjef Åsmund Weltzien i NUPI understreker at instituttet har gått grundig gjennom sine sikkerhetssystemer etter spion-angrepet. FOTO: MATTIS SANDBLAD, VG

Hentet fra: Nyhetssaker på nett

Situasjonsbildet

NorSIS sitt mål er at alle skal ha en trygg digital hverdag. En digital hverdag er etterhvert blitt vanlig. Digitale løsninger er ikke et mål i seg selv, men et middel som skaper verdi og bidrar til økt velferd i hele samfunnet. En økende avhengighet til digitale løsninger gjør imidlertid samfunnet mer sårbart. De digitale tjenestene blir kritiske for at samfunnet skal kunne fungere normalt og åpner for nye og endrede sårbarheter. Jo mer bevisste vi er, også om baksiden av den digitale medaljen, desto bedre kan vi beskyttes oss – mot egne feil og mot cyberkriminelle som er ute etter verdiene våre.

Kunnskap og kultur

NorSIS er grunnleggende positiv til digitalisering, med løsninger som gjør hverdagen lettere og samfunnet tryggere. Derfor er det så viktig for oss å bevisstgjøre så mange som mulig også om ulempene – for å dempe usikkerhet og motvirke uvilje til å ta nye muligheter i bruk.

Samfunnet stilles ovenfor nye utfordringer knyttet til digitalisering og autonome systemer. Førerløse biler skaper bedre trafikksikkerhet, men øker sårbarheten for at andre kan ta over kontrollen av bilen. I tillegg kommer alle de juridiske aspektene ved slike systemer, hvordan bilen skal agere i gitte situasjoner. Det hevdes av enkelte at de første som ikke behøver ta førerkort allerede er født.

Datakriminalitet skaper utfordringer utover landegrenser, da kriminalitet over nettet kan gjøres fra alle deler av verden. Dette skaper utfordringer for myndigheter, virksomheter og privatpersoner. Trussel-, kriminalitets- og sårbarhetsbildet endrer seg raskt; raskere enn både myndigheter, virksomheter og privatpersoner makter å respondere.

Vi kan aldri sikre oss mot alle truslene. Kompetanse og kunnskap om trusler og sårbarheter gjør oss imidlertid bedre i stand til å beskytte våre verdier. Og vi kan lære oss å leve med et akseptabelt – og akseptert – risikonivå. Slik bevissthet, med basiskunnskap og sikkerhetskultur som bidrar til en tryggere digital atferd, forutsetter en viss kjennskap til truslene og forståelse for trendene. «Trusler og trender» er et viktig verktøy for virksomheter og privatpersoner slik at de kan øke sin bevissthet og samtidig redusere sårbarheter.

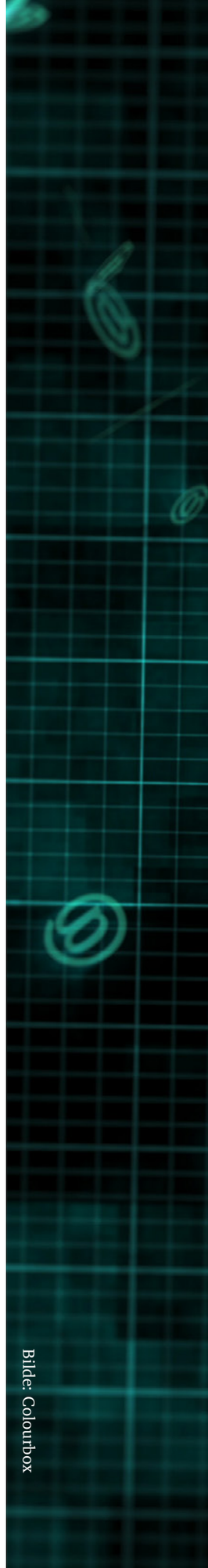
Individer og virksomheter

Faren for å bli utsatt for nettbasert kriminalitet, både mot privatpersoner og virksomheter, vil kunne øke. Den raskt voksende trenden med Tingenes internett forsterker dette. Når vi kobler stadig digitale enheter til nettet, øker sårbarhetene. Utviklingen krever kunnskap, men også samarbeid mellom offentlige og private aktører slik at vi er best mulig rustet til å beskytte oss og bidra til at alle kan ha en trygg digital hverdag.

Peggy S. Heie
Administrerende direktør, NorSIS

TRUSLER

2017–18



Bilde: Colourbox

Trusselbildet

Informasjonstyveri

Beskrivelse: Målet utsettes for tyveri av person- eller bedriftsinformasjon. Metoden er typisk datainnbrudd og nettfisking, falske apper og nettsider, søppelsnoking og hacking av tredjeparter.
Trusselaktør: Kriminelle.
Mål: Privatpersoner, virksomheter.

Vanvare

Beskrivelse: En selv utsetter seg eller bedriften for risiko. Vanvaren er typisk ubetenksomhet, bl.a. som følge av for lav bevissthet eller manglende kunnskap.
Trusselaktør: En selv.
Mål: Privatpersoner, virksomheter.

Løsepengevirus

Beskrivelse: Målet presses for penger; oftest ved at filer krypteres, og det kreves løsepenger for å låse dem opp igjen. Metoden er spredning av skadevare, oftest via falsk e-post eller pop-ups på nettsider. Noen ganger utnyttes sikkerhetshull i programvare til å spre skadevaren.
Trusselaktør: Kriminelle.
Mål: Privatpersoner, virksomheter.

Direktørsvindel

Beskrivelse: Målet svindles for penger; ved at de kriminelle utgir seg for å være en toppsjef som instruerer en rask utbetaling. Metoden er særlig falsk e-post, SMS, med kartlegging av virksomhet og interne rutiner og sosial manipulering av en betrodd medarbeider.
Trusselaktør: Kriminelle.
Mål: Virksomheter.

Industrispionasje

Beskrivelse: Målet utsettes for tyveri av sensitiv forretningsinformasjon; enten fra en stat, kriminelle eller konkurrenter. Metoden er f.eks. spionvare og sosial manipulering, insidere og bruk av småbedrifter som brohoder.
Trusselaktør: Kriminelle, stater, virksomheter.
Mål: Virksomheter.

Sabotasje

Beskrivelse: Målet utsettes for fysisk eller digital sabotasje; ved hjelp av digitale angrep for å ødelegge eller for å påvirke. Metoden kan ofte være tjenestenektangrep, og spam med spredning av skadevare.
Trusselaktør: Kriminelle, stater, vandaler og aktivister.
Mål: Virksomheter.

Identitetstyveri

Beskrivelse: Målet utsettes for ID-tyveri og misbruk av identitet, som brukes til svindel. Metoden er typisk datainnbrudd eller -snoking, med nettfisking som utbredt metode med flere varianter.
Trusselaktør: Kriminelle.
Mål: Privatpersoner, (virksomheter).

Datingsvindel

Beskrivelse: Målet svindles for penger; oftest ved at angriper bygger en falsk kjærlighetsrelasjon og utnytter opparbeidet tillit ved å be om penger. Metoden er typisk bruk av sosiale medier, falske identiteter, oppdiktede historier og sosial manipulering.
Trusselaktør: Kriminelle.
Mål: Privatpersoner.

Personutpressing

Beskrivelse: Målet presses for penger eller tjenester; ofte ved trussel om å spre sensitiv eller intim informasjon. Metoden kan være kapring av konto ved hjelp av nettfiske (phishing), og annen form for sosial manipulering, deling av bilder og opptak av video-samtaler.
Trusselaktør: Kriminelle, inkl. overgripere.
Mål: Privatpersoner.

Krenkelser

Beskrivelse: Målet utsettes for trakassering; bl.a. ved digital sjikane og mobbing, eller overgrep av seksuell karakter. Metoden er spredning av falske påstander, bilder og video eller å forlede offeret inn i krenkende situasjoner.
Trusselaktør: Overgripere og plageånder.
Mål: Privatpersoner.

NorSIS har valgt ut ti trusler som rammer norske privatpersoner og virksomheter. Metodikken er redegjort for på side 17. Truslene er ikke rangert etter alvorlighet.

Trusselbeskrivelse

Informasjonstyveri

Beskrivelse

Trusselaktørene er i hovedsak kriminelle, som samler og systematiserer informasjon om personer eller virksomheter som så brukes i annen kriminell virksomhet. Stjålet informasjon kan brukes som et instrument i f.eks. utpressing, svindel og krenkelser, spionasje og sabotasje. Informasjonstyveri tyveri rettet mot bedrifter har likhetstrekk med industrispionasje. Informasjonstyveri rettet mot privatpersoner kan føre til identitetskrenkelser.

Metodene som brukes er mange, framfor alt ulike typer nettfisking (phishing) med e-post eller SMS (smishing), samt tilsvarende og avanserte metoder rettet spesielt mot utvalgte bedrifter eller personer (spear phishing), så vel som innbrudd (hacking). I tiltagende grad blir falske apper brukt til å samle inn informasjon, og legitime apper kan hackes til å avgi informasjon. Bruk av skadevare er også vanlig, spredd via e-post og falske nettsider. Datalekkasjer hos tjenesteleverandører kan medføre at brukerdata kommer på avveier og søppelsnoking fra avhendede (eller stjålne) digitale enheter kan også føre data på avveier.

Alvorlighet

Omfanget er ikke kjent, men antas å være stort. Alvoret ligger mest i at stjålet informasjon brukes som et middel og til dels er en forutsetning for iverksetting av andre trusler.

Konsekvensene kan være store ved bruk i ulike typer angrep, inkl. ID-tyveri og svindel, krenkelser og utpressing. Person- eller virksomhetsinformasjon på avveier øker sårbarheten for å bli angrepet, og for å miste materielle og immaterielle verdier.

Tiltak

Viktigst for å forhindre tyveri er grunnleggende informasjonssikkerhet med gode rutiner for adgangskontroll, oppdateringer, kryptering, sikker sletting av data, og stor aktsomhet overfor lenker og vedlegg i e-post.

Det er viktig å sikre brukerkontoer på nett ved å følge rådene for sikker pålogging. Ta i bruk to-trinns bekreftelse på alle tjenester hvor det er mulig, og bruk unike passord på alle tjenester.

For større virksomheter med egen IT-avdeling, og leverandører av IT-tjenester, vises til anbefalte tiltak fra NSM for grunnsikring mot skadevare. Sikkerhetsovervåking anbefales for å oppdage hendelser og begrense skade, samt sikkerhetstesting for å bekrefte at sikkerhetsbarrierer og sikkerhetsovervåking fungerer som tiltenkt.

Les mer: *nettvett.no/sikker-palogging*
Les mer: *nsm.stat.no/virksomhetssikkerhet/fire-enkle-tiltak-stopper-90-prosent-av-dataangrep/*

Vanvare

Beskrivelse

Trusselaktøren kan i noen tilfeller være oss selv. Uheldige valg og vurderinger tatt av mennesker med gode intensjoner kan like gjerne som teknologiske og organisatoriske brister, føre til at informasjon kommer på avveier eller blir utilgjengelig. Økt bruk av ny teknologi og nettverkstilkoblede enheter øker sårbarheten, og faren for å gjøre feil. Kompleksiteten øker og det krever større kunnskap og skjerpet bevissthet for å redusere risikoen for at en selv i vanvare bidrar til at andre trusler slår inn.

Metodene er egne uheldige handlinger basert på manglende kunnskap og bevissthet om digitale trusler. Med vanvare menes f.eks. at man tar i bruk ny teknologi uten å sette seg inn i konsekvensene den har for informasjonssikkerheten. Det kan gi utslag i at man eksempelvis unnlater å bytte standardpassord på en internett-tilkoblet enhet, synkroniserer data til skyen uten å være klar over det eller andre feilkonfigurasjoner. Med lav bevissthet rundt digitale trusler er man gjerne også mer sårbar for sosial manipulering.

Alvorlighet:

Omfanget må formodes å være betydelig, idet de fleste vil stå i fare for å gjøre feilvurderinger, med de følger det kan ha.

Konsekvensen kan være mangfoldig, og åpne for at ulike aktører lettere får gjennomført sine forsett, og at enkeltpersoner og virksomheter lettere blir utsatt for digital kriminalitet eller trakassering. At informasjon blir utilgjengelig, endret eller kommer på avveier er også en sannsynlig konsekvens.

Tiltak

Viktigst for å unngå å gjøre feil som kan skade en selv eller virksomheten, er grunnleggende kunnskap om informasjonssikkerhet og en kultur for å spørre om råd og hjelp.

Les mer: *nettvett.no/nettvettreglene*

Løsepengevirus

Beskrivelse

Trusselaktørene er kriminelle som forsøker å presse privatpersoner og virksomheter til å betale løsepenger etter først å ha gjort filer utilgjengelig f.eks. ved bruk av kryptering, med trussel om å offentliggjøre eller ødelegge data hvis avkrevde løsepenger ikke blir betalt. De fleste løsepengevirus (ransomware) krypterer informasjonen på maskin og i nettverk, men lar selve enheten virke samtidig som det fremmes krav om løsepenger for at eieren skal få tilbake tilgangen. Det trues ofte med at betaling må skje raskt for at informasjon ikke skal bli ødelagt eller at beløpet skal øke. Utpresserne vil gjerne ha betaling i en kryptovaluta, typisk Bitcoin, for å dekke sporene sine.

Metoden er typisk spredning av skadevare via vedlegg i e-poster og SMS, Office-filer, eller fra infiserte nettsider. E-post er den klart mest brukte metoden. Det finnes en rekke typer slike virus. Blant de mest kjente er WannaCry, Petya/NotPetya og Cryptolocker.

Alvorlighet

Omfanget er ikke kjent, men bl.a. basert på rapporter om større angrep, synes trusselen å være tiltagende. Dette er også en enkel og billig måte å gjennomføre massive angrep på, med rask spredning til store mottakergrupper, og med liten fare for å bli tatt. Internasjonalt regnes løsepengevirus som en topp-trussel, med størst vekst av alle. Dette bekreftes også av Europol.

Konsekvensen for de som rammes vil først og fremst være økonomisk tap, eller tap av data. For virksomheter kan tap av data ha negativ innvirkning på tilliten i markedet, mens for privatpersoner kan affeksjonsverdien være like viktig.

Tiltak

Det viktigste forbyggende tiltaket er å ha gode rutiner for sikkerhetskopiering og testing av denne. De kriminelle mister da sitt pressmiddel mot virksomheten. Brukere med bevissthet om falske e-poster med skadelige lenker og vedlegg kan unngå å bli rammet. Oppdatert operativsystem og programvare (inkl. antivirus) kan i noen tilfeller stoppe skadevaren.

For større virksomheter med egen IT-avdeling, og leverandører av IT-tjenester, vises til anbefalte tiltak fra NSM for grunnsikring mot skadevare. Sikkerhetsovervåking anbefales for å oppdage hendelser og begrense skade, samt sikkerhetstesting for å bekrefte at sikkerhetsbarrierer og sikkerhetsovervåking fungerer som tiltenkt.

Les mer: *nettvett.no/losepengevirus*
Les mer: *nsm.stat.no/virksomhetssikkerhet/fire-enkle-tiltak-stopper-90-prosent-av-dataangrep/*

Direktørsvindel

Beskrivelse

Trusselaktørene er kriminelle som utgir seg for å være en toppleder (gjerne direktør eller økonomidirektør). Ved direktørsvindel (CEO-fraud) sendes det falske meldinger med beskjed om å gjennomføre utbetalinger adressert til personer med betalingsfullmakter i bedriften. Den første meldingen følges gjerne opp med en instruks om utbetaling til et oppgitt kontonummer som tilhører svindlerne. Svindlerne videresender pengene via flere konti for å skjule transaksjonene. Slike svindler rammer både store og mindre virksomheter.

Metoden er falsk e-post og/eller SMS, utgitt for å være sendt fra en av selskapets toppledere, gjerne fulgt opp av en telefonhenvendelse. Falske e-faktura er også brukt. Et godt forberedt angrep vil ofte inkludere kartlegging av selskapets ledelse, rutiner og aktivitet. Meldinger har gjerne et språk som til forveksling ligner språket til den påståtte avsenderen. I tillegg opprettes det gjerne et domene for å etterligne bedriftens e-postadresser, eller e-postadressene kan være forfalsket. Det er også eksempler på at brukerkonti er overtatt, og at falske meldinger sendes fra en ekte konto.

Alvorlighet

Omfanget er merkbart, også i Norge, med kjente angrep rettet mot både store og mindre virksomheter, samtidig som det er mørketall. Alvoret for de som blir svindlet avhenger både av hvor mye penger som tapes, og hvordan omdømmet påvirkes.

Konsekvensen kan være alvorlig, med store økonomiske tap, i verste fall konkurs.

Tiltak

Viktigst for å forhindre svindel er gode interne rutiner og kontroll ved utbetalinger som avviker fra normalen, gjerne med personlig avsjekk (per telefon/SMS) med den som står som avsender.

For større virksomheter med egen IT-avdeling, og leverandører av IT-tjenester, vises til anbefalte tiltak fra NSM for grunnsikring mot skadevare. Sikkerhetsovervåking anbefales for å oppdage hendelser og begrense skade, samt sikkerhetstesting for å bekrefte at sikkerhetsbarrierer og sikkerhetsovervåking fungerer som tiltenkt.

Les mer *nettvett.no/direktor-svindel*
Les mer: *nsm.stat.no/virksomhetssikkerhet/fire-enkle-tiltak-stopper-90-prosent-av-dataangrep/*

Industrispionasje

Beskrivelse

Trusselaktørene er oftest kriminelle eller stater, men også konkurrenter. Verdien av sensitiv informasjon avhenger av motiv og bruk. En angriper vil søke informasjon som har stor strategisk og kommersiell verdi for det angrepne selskapet, evt. også av sikkerhetsverdi for land dette opererer i og leverer til. Sistnevnte kan typisk dreie seg om forsvars- eller annen høyteknologisk industri som særlig ikke-allierte stater har interesse av.

Metoden kan være spionvare (spyware) spredt via vedlegg til e-post eller falske nettsider (vannhull), ved bruk av sosial manipulering og insidere. Det siste kan skje ved at ansatte presses eller forledes til å gi angriperne adgang til informasjon. Ofte angripes underleverandører, hvilket gjør også mindre bedrifter utsatte, fordi de sitter på sensitiv informasjon eller er brohoder inn mot sin kunde eller oppdragsgiver.

Alvorlighet

Omfanget er uklart, men spionasje må antas å forekomme. Norske sikkerhetsmyndigheter advarer mot spionasje fra fremmede makter.

Konsekvensen kan være svært alvorlig, både for en virksomhet og en stat. Et selskap kan påføres store økonomiske tap, og alvorlig tap av tillit og anseelse. En stat risikerer at sensitiv informasjon på avveie svekker rikets sikkerhet, eller også samfunnssikkerheten.

Tiltak

Viktigst for å forhindre spionasje er samme forholdsregler som for informasjonstyveri, med gode rutiner og sikker atferd, samt kryptering av sensitiv informasjon. En viktig erkjennelse er at alle kan være et mål.

For større virksomheter med egen IT-avdeling, og leverandører av IT-tjenester, vises til anbefalte tiltak fra NSM for grunnsikring mot skadevare. Sikkerhetsovervåking anbefales for å oppdage hendelser og begrense skade, samt sikkerhetstesting for å bekrefte at sikkerhetsbarrierer og sikkerhetsovervåking fungerer som tiltenkt.

Les mer: *nsm.stat.no/virksomhetssikkerhet/fire-enkle-tiltak-stopper-90-prosent-av-dataangrep/*
Se også: *nettvett.no/ikt-utenfor-kontoret*

Sabotasje

Beskrivelse

Trusselaktørene kan være kriminelle, aktivister og vandaler, så vel som fremmede stater. Sabotasje gjennom digitale midler kan lamme en virksomhet med nedetid eller også påføre den fysisk skade. Sabotasjen kan iverksettes rett og slett for å ødelegge, eller som et ledd i et sammensatt angrep, inkl. såkalte hybride angrep som har politiske motiver.

Metodene kan ofte være tjenestenektangrep (DDoS) og spredning av skadevare som påvirker en komponent eller en prosess.

Alvorlighet

Omfanget er ukjent, men det er ikke usannsynlig at også norske virksomheter, i Norge eller utlandet, kan bli utsatt for sabotasje.

Konsekvensen kan være alvorlig både for den enkelte virksomhet og for samfunnet. Virksomheten kan lide avgjørende økonomiske tap, så vel som tapt anseelse og tillit. Samfunnets sikkerhet kan svekkes hvis f.eks. samfunnskritisk infrastruktur settes ut av funksjon.

Tiltak

Viktigst for å forhindre sabotasje er samme forholdsregler som for spionasje, med gode sikkerhetsrutiner og sikker atferd, samt en robust infrastruktur.

For større virksomheter med egen IT-avdeling, og leverandører av IT-tjenester, vises til anbefalte tiltak fra NSM for grunnsikring mot skadevare. Sikkerhetsovervåking anbefales for å oppdage hendelser og begrense skade, samt sikkerhetstesting for å bekrefte at sikkerhetsbarrierer og sikkerhetsovervåking fungerer som tiltenkt.

Les mer: *nsm.stat.no/virksomhetssikkerhet/fire-enkle-tiltak-stopper-90-prosent-av-dataangrep*
Se også: *nettvett.no/ddos-angrep*

Identitetstyveri

Beskrivelse

Trusselaktøren er kriminelle som ser verdien i å anskaffe, overføre, besitte eller fremstå som rette innehaver av personlige opplysninger tilhørende en privatperson eller selskap på en uautorisert måte, med den hensikt å begå bedrageri eller annen kriminalitet. Identitetssvindel er ervervelse av penger, varer, tjenester og andre fordeler eller unngåelse av økonomiske eller andre forpliktelser ved å utgi seg for å være en annen ved bruk av falsk identitet. En vanlig svindelform er at en kriminell benytter en annen persons reelle eller fiktive e-postadresse, bostedsadresse, telefonnummer eller personnummer for å kjøpe varer på internett.

Metodene for å skaffe til veie personlige opplysninger er de samme som beskrevet under avsnittet om informasjonstyveri. Kartlegging gjennom sosiale medier og åpne kilder er også vanlig.

Alvorlighet

Omfanget av ID-tyveri i en eller annen form er stort, og synes å berøre stadig flere. En årlig NorSIS-undersøkelse indikerer at ca. 170.00 personer over 18 år er rammet over en periode på de to siste årene. Enkeltsaker kan være svært belastende, særlig for privatpersoner.

Konsekvensen vil kunne være økonomisk tap og gjentagende misbruk av personens identitet. Misbruk kan medføre betydelige ulemper for den som blir rammet, inkl. svertet omdømme. Opprydding kan være tidkrevende – og psykisk belastende, bl.a. ved at offeret ikke blir trodd, og må bevise sin egen uskyld.

Tiltak

Viktigst for å forhindre ID-tyveri er å sikre digitale enheter og brukerkontoer på nett mot uautorisert tilgang. I tillegg bør man være forsiktig med å gi fra seg personlige opplysninger.

Les mer: *nettvett.no/forebygge-identitetsverdi*

Datingsvindel

Beskrivelse

Trusselaktørene er kriminelle som utgir seg for å være en respektabel person, eksempelvis en offiser eller forretningsmann, ofte fra USA – eller også fra Norge. Vedkommende ønsker kontakt, og hevder etter hvert å trenge hjelp. Det spilles på offerets livssituasjon og sårbarhet, og det etableres et tillitsforhold som oftest utvikles til en romantisk relasjon. Forut for et avtalt møte trenger personen plutselig penger for å kunne komme; deretter oppstår nye vanskeligheter, med behov om nye pengeoverføringer.

Metoden er bruk av sosiale medier og utspekulert sosial manipulering. Etter opprettet kontakt i ulike fora vil svindleren føre kontakten over til mer private kanaler; e-post eller en chattetjeneste – ved hjelp av falske profiler. Det bes gjerne først om mindre beløp før summene øker, gjerne i sammenheng med tåredryppende historier om sykdom eller familiære kriser. Tillitsforholdet bygges ofte opp over flere måneder eller år. Angrep rettes særlig mot godt voksne; som med profiler i sosiale medier avdekker sin sivile situasjon. Kriminelle leter etter ofre på datingsider og sosiale medier.

Alvorlighet

I Norge har antall tilfeller registrert av Politiet ligget på ca. 100–200 i året, med samlede utbetalinger på over 200 millioner kroner, men det er trolig store mørketall. Følgene kan bli svært alvorlige for de som blir svindlet; med i verste fall stor gjeld og svekket selvbilde.

Konsekvensen vil være økonomisk tap, men kan også føre til psykiske utfordringer i møte med tabuer, sorg og skam. Ofrene vil oftest ikke fortelle om eller anmelde saken.

Tiltak

Bevissthet rundt denne formen for svindel kan gjøre den mulig å oppdage. Om noen man chatter med ber om penger, søker privat informasjon, er veldig opptatt av å bygge tillitt og er pågående bør man være skeptisk.

Er man utsatt for datingsvindel er det viktig å slutte og gjennomføre utbetalinger. Saken bør anmeldes til politiet og banken bør kontaktes dersom man har gitt fra seg informasjon som kan gjøre at svindleren kan tappe en for ytterligere verdier.

Les mer: *nettvett.no/datingsvindel*

Personutpressing

Beskrivelse

Trusselaktørene er vinningskriminelle eller overgripere som samler sensitivt materiale om en person, særlig intime bilder eller videoer, for å bruke dette til utpressing. Materialet blir brukt til å kreve penger, nakenbilder eller annet, under trussel om at bilder eller opptak vil bli spredt på nett. Angriperne er ute etter penger eller tjenester av seksuell karakter, eller vil hevne og hevde seg. Bilder og video kan være laget og delt frivillig av offeret, eller spredd av andre, da oftest uten samtykke. Video-opptak gjøres ofte uten at offeret er klar over det. Utpresseren kan typisk true med å spre et relativt uskyldig nakenbilde hvis ikke offeret gir fra seg nye og mer eksplisitte bilder, eller utfører seksuelle handlinger f.eks. på Skype – som så tas opp og brukes til mer utpressing. Henvendelser til Slettmeg.no tyder på at videoutpressing oftest rammer voksne menn, mens utpressing med nakenbilder oftest rammer ungdom, mest jenter.

Metodene som brukes for å få tak i f.eks. private bilder kan være kapring av offerets skykonto ved hjelp av nettfiske (phishing). Dette kan også skje om noen snoker på en ulåst mobil, eller om man har delt passordet sitt med vedkommende. Noen blir også overtalt med smiger til å sende intime bilder, og deretter flere og mer detaljerte bilder eller opptak, også ved bruk av trusler. Grensen mellom utpressing og overgrep er flytende.

Alvorlighet

Omfanget er ikke stort, men konsekvensen kan være svært alvorlig for offeret, både økonomisk, psykisk og sosialt. Fordi dette også rammer unge som ikke ser konsekvensene av det som skjer, og som er i en sosialt sårbar alder, er denne typen kriminalitet ekstra alvorlig. Både for den enkelte og samfunnet. Ofrenes rettssikkerhet trues også fordi de ofte ikke tør å si fra til voksne, eller anmelde saken.

Tiltak

Det er viktig å spørre seg selv om hvilke motiver folk kan ha for å ta kontakt på nett. Om man blir utsatt for personutpressing er det viktig å søke hjelp og snakke med noen. Utpressing er en kriminell handling og bør anmeldes til politiet.

Det er viktig å sikre brukerkontoer på nett ved å følge rådene for sikker pålogging. Ta i bruk totrinns bekreftelse på alle tjenester hvor det er mulig, og bruk unike passord på alle tjenester. Man kan gjerne benytte et passordhåndteringsprogram, eller skrive ned passordene og oppbevare dem trygt og hemmelig. Det er viktig at alle lærer seg at passord er private, og ikke skal deles med andre.

Les mer: *nettvett.no/sikker-palogging*

Krenkelser

Beskrivelse

Trusselaktørene er ulike med forskjellige hensikter, og ikke alle er kriminelle. Krenkelser består av to hovedkategorier: Trakassering og overgrep. Det første kan ende med det siste, som er det klart alvorligste – og utvilsomt kriminelt. Trakassering kan bestå av digital mobbing: i en lukket kanal overfor offeret eller med åpen uthenging. Overgrep er særlig knyttet til seksuelle handlinger framtvunget over nett, med seksualisert språkbruk, og som kan føre til fysiske møter og overgrep. Trakassering og overgrep kan ramme begge kjønn og alle aldre, men barn og ungdom er særlig utsatt.

Metoder for trakassering er typisk konstruksjon og spredning av ondsinnede karakteristikker og falske påstander, anonymisert mobbing med apper som Sarahah, og deling av bilder og filmer via sosiale medier. Overgrep bygger som regel på sosial manipulering, med overtalelse og trusler, og forledelse og utpressing av offeret, som så går med på en uønsket, ufrivillig handling. Barns ukritiske bruk av sosiale medier er påpekt som én måte å lokke barn (og andre) i situasjoner som i verste fall kan føre til voldtekt. Spredning av seksualiserte bilder og filmer uten de medvirkende sin vitende og vilje er også overgrep.

Alvorlighet

Omfanget er uklart, men henvendelser til Slettmeg.no gir en god pekepinn, med ca. 1500 per år. Følgene kan være svært alvorlige, både av trakassering og overgrep. Konsekvensene kan gå på psykisk helse (og i verste fall livet) løs. Sosiale relasjoner kan bli påvirket, der også tredjeparter (f.eks. familie) kan bli skadelidende.

Tiltak

Det er viktig å søke hjelp fra noen man stoler på om man blir utsatt for trakassering eller overgrep. Alvorlige forhold bør anmeldes til politiet. Det er viktig å senke terskelen for når barn og ungdom sier ifra. Om man har barn bør man ta samtalen om at de kan komme til deg hvis de opplever noe ubehagelig på nett.

All datakriminalitet bør anmeldes.
Se veiledning på Nettvett.no

Trusselvurdering

De ti truslene som er beskrevet har vært gjennomgående i 2017, men antas å ville prege bildet i 2018 også. Dette er trusler rettet både mot privatpersoner og virksomheter. Følgene vil variere, men oppleves som regel alvorlig for de som rammes. Det kan være økonomiske tap, tap av omdømme, eller innebære personlige konsekvenser.

Norge er et av de mest digitaliserte landene i verden. Det kan medføre større sårbarhet, men også bidra til større sikkerhet. Nytt utstyr, oppdatert programvare og gode sikkerhetsrutiner vil gi god beskyttelse, og sjansene for at angrep skal lykkes blir mindre. NSM[1] ser imidlertid et økende gap mellom behov for og tilgjengelighet av sikkerhetskompetanse, noe som utgjør en nasjonal sårbarhet. Tjenesteutsetting av IKT-tjenester til profesjonelle aktører kan bøte på denne utfordringen og bidra til bedre sikring av virksomheters nettverk og verdier.

Det overordnede digitale trusselbildet endrer seg ikke raskt. De samme hovedtruslene går gjerne igjen fra ett år til det neste. Metodene som brukes for å iverksette angrep, for å nå målet og komme til verdiene, endrer seg derimot kontinuerlig. Dette er et kappløp mellom kriminelle på den ene siden og sikkerhetsselskaper og myndigheter på den andre. De mest profesjonelle cyberkriminelle blir stadig mer sofistikerte, og utvikler nye metoder som gjør truslene like aktuelle. Internasjonal, organisert kriminalitet har flyttet seg til cyberdomenet, i takt med global digitalisering. Her finner de gode muligheter til vinning – med relativt små investeringer og liten risiko. Enkelte trusler, som løsepengevirus, har en forretningsmodell som stadig utvikles og datakriminalitet har blitt en tjeneste (Crime as a Service – CaaS). Digitale kriminelle verktøy er en global handelsvare, slik persondata for lengst er blitt det.

Valg av trusler

Trusselvurderingen er gjennomført med tanke på små- og mellomstore bedrifter og privatpersoner. Mange av disse truslene gjelder også store selskaper og statlige virksomheter. Angrep mot disse vil mest sannsynlig også ha innvirkning på de mindre aktørene. Digitale trusler kjenner ingen landegrenser. Kriminelle aktører er anonyme, opererer internasjonalt og skjuler seg godt i et globalt miljø på nett. Plageånder og overgripere opererer gjerne anonymt eller med en fiktiv identitet.

40 % av de spurte oppgir å ha blitt lurt til å gi fra seg privat informasjon, og 8 % arbeidsrelatert informasjon gjennom nettfisking (phishing). 12 % har opplevd innbrudd i sin private e-post eller private kontoer i sosiale nettverk. Over 60 % svarer at det er krevende å beskytte seg selv mot svindel og annen type datakriminalitet.
Telenor: Digital sikkerhet 2017

Konsekvensene fra de fleste angrep er sammensatte, både for privatpersoner og virksomheter. Trusselaktører er ofte ute etter verdier for vinnings skyld og ofrene kan lide økonomiske tap. Men for mange, individer som selskaper, vil også tap av omdømme – tillit og anseelse – være alvorlig. For enkeltpersoner kan det medføre ødelagte sosiale relasjoner og psykologiske vansker; for bedrifter kan tillitstap også få økonomiske følger. Konsekvenser for samfunnet kan være at opplevd usikkerhet fører til at folks tillit til digitale løsninger svekkes.

Flere faktorer har vært lagt til grunn i utvelgelsen av truslene. En trussel skal være sannsynlig, og ha et betydelig skadepotensial – enten ved å ramme mange, eller at de som blir angrepet rammes hardt.

Trusler i arbeidslivet

NorSIS får et godt bilde på hva som preger trusselbildet i næringslivet gjennom direkte henvendelser og tjenesten Nettvett.no. Dette har i 2017 særlig vært direktørsvindel og utpressing med løsepengevirus. Direktørsvindel er vanlig og rammer norske bedrifter. Internasjonale sikkerhetsaktører som McAfee og Trend Micro melder i sine rapporter at løsepengevirus også vil være en stor trussel i 2018[2]. Enkelte peker også på sabotasje som en reell trussel, i tillegg til spionasje.

Informasjonstyveri er en stor trussel for alle virksomheter. Ofte kan det være vanskelig å vurdere det eksakte tapet av verdi som virksomhetene mister. Informasjonstyveri fra virksom-

[1] NSM: Helhetlig IKT-risikobilde 2017

[2] Trend Micro Security Predictions for 2018.

heter vil også være en potensiell risiko for privatpersoner hvis det er personinformasjon som blir frastjålet. De mest pålitelige og seriøse virksomheter vil utsettes for fare for tap av omdømme og tillit grunnet det omfang og den omstillingstakten som informasjonssikkerhetstrusler utgjør i dag, melder Information Security Forum[3]. Foreningen melder at 2018 vil være et år hvor vi ser sofisitikerte trusler og trusselaktører som tilpasser sine metoder til målgruppens svake punkter og tilpasser angrepsmetoder slik at de tar hensyn til forsvarstiltak som allerede er iverksatt.

61 % av spurte danske og norske bedriftsledere er mer bekymret for cyberkriminalitet i 2017 enn året før, og 52 % av virksomhetene var utsatt for hendelser knyttet til slik kriminalitet. Men bare 33 % forventer økte budsjetter for informasjonssikkerhet neste år, og kun15 % vurderer kunnskapsmangel i ledelsen som en trussel.

PWC: Cybercrime Survey 2017

Norske høyteknologiske virksomheter kan også være attraktive mål for statlige makter. PST[4] melder i sin trusselvurdering for 2017 at Norge og norske interesser vil utsettes for fremmed etterretningsvirksomhet som kan ha et stort skadepotensial. Aktiviteten vil blant annet rettes mot mål innenfor norsk forsvars- og beredskapssektor samt mot politiske beslutningsprosesser og kritisk infrastruktur. Fremmede tjenester bruker både avanserte datanettverksoperasjoner og tradisjonelle metoder mot norske mål. Dette betyr at også underleverandører til disse virksomhetene kan være mål, enten direkte eller indirekte. Alle små – og mellomstore bedrifter har verdier som kan angripes, enten det er i kraft av sin egen virksomhet, eller som en underleverandør for andre selskaper når de inngår i stadig mer komplekse og globale, verdi- og leveransekjeder.

93 % av respondentene i norsk næringsliv oppgir at de ikke har blitt utsatt for digitale sikkerhetshendelser, med tap, siste år. Datavirus oppgis samtidig som den største digitale sikkerhetsutfordringen (55 %), mens dataangrep anses som den mest kritiske hendelsesrisiko. Bare 39 % inkluderer informasjons- og IKT-sikkerhet i sin risikostyring.

BDO: Risikoundersøkelsen 2017

Ti trusler er valgt, flere kunne vært med. Blant annet utsettes vi for tiltagende uønsket påvirkning, særlig gjennom sosiale medier. En av teknikkene som brukes er falske nyheter. En annen trussel å være oppmerksom på er den omfattende innsamlingen av personopplysninger om oss; med eller uten vårt samtykke. Til dette brukes eksempelvis konkurranser på nettet, både ekte og falske. Persondata er en salgsvare, og kan misbrukes på flere vis – fra tilpasset reklame til målrettet kriminalitet.

Trusler i privatlivet

NorSIS får et godt bilde på hva som preger trusselbildet for privatpersoner gjennom tjenestene Slettmeg.no og Nettvett.no. Mange av de som kontakter Slettmeg.no er i en krise. Enten ved at de har gjort noe de angrer på, eller at noen har gjort noe mot dem. Mange bruker lang tid på å søke hjelp, eller vegrer seg for å gjøre det, noe som indikerer mørketall. Krenking på nett, framfor alt på sosiale medier, er utbredt – og farlig. Kyniske mobbere og overgripere bruker sosial manipulering for å vinne fram – og ødelegge. Dette er også en av få trusler der økonomisk vinning ikke er drivkraften, men hvor konsekvensen kan være mer dramatisk.

Mange trusler kan ramme individer både privat og på jobb eller virksomheten. Dette forsterkes av at skillet mellom arbeid og fritid stadig blir mindre tydelig og man benytter de samme digitale enhetene og tjenestene begge steder. Det gjelder særskilt skyløsninger og Tingenes internett (IoT), som vokser i utbredelse og bruk. Både skytjenester og IoT kan for mange øke sikkerheten, men brukerne må også forholde seg til nye sårbarheter.

[3] infosecurity-magazine.com/news/isf-top-2018-threats

[4] PST: Trusselvurdering 2017

Bilde: Colourbox

Digitalt samfunn, sosial manipulering

Sosiale medier er for mange en viktig del av den digitale hverdagen. Sosial manipulering er en del av digitaliseringens skyggeside. Digitalisering er verdifull; manipulering ødeleggende.

Kriminelle er kyniske. De vet hva de er ute etter, og de bruker en rekke metoder for å nå sine mål. Sosial manipulering er en mye brukt metode innenfor flere av truslene beskrevet i denne rapporten, i spennvidden industrispionasje til personovergrep, og mest av alt: ulike typer svindel og utpressing. Fellesnevneren er å manipulere et menneske, enten offeret selv, eller en person som misbrukes for å nå verdiene de kriminelle er ute etter. Mens en del trusler domineres av tekniske teknikker, som automatisk spredning av skadevare, er dette en metode som rammer mennesker direkte. Andre metoder er teknologisk basert, mens dette er psykologisk fundert. Manipulatorene spiller særlig på fristelser, frykt og tillit for å nå fram. De har typisk en sosial evne til å vinne tillit hos fremmede, og til å overtale. De utnytter menneskelig sårbarhet, og klarer derved å omgå teknisk beskyttelse. Slike angrep rettes mot enkeltindivider, som manipuleres (overtales, misledes, trues), til å gi fra seg noe, oftest motvillig eller ufrivillig. Eller de gjør det i god tro, etter å ha blitt lurt.

Metoden utnytter den raske digitaliseringen, som i Norge har kommet lenger enn i de fleste land. Det inkluderer utstrakt, og stigende, bruk av sosiale medier. Ifølge SSB brukte 65 % av den voksne befolkningen slike medier daglig i 2017, mot 54 % året før. Ca. 85 % bruker e-post, som er et viktig medium for manipulasjon. Barn og unge bruker også i stor utstrekning sosiale medier, inklusive apper. Samme verktøy brukes også til digital mobbing. Tall fra Medietilsynet (2016) viser at 80 % av unge i alderen 9–16 år bruker Snapchat; 76 % Instagram. Andelen som har opplevd mobbing har vært økende fra år til år. Veiledningstjenesten Slettmeg.no sitter på alarmerende dokumentasjon om denne skyggesiden av digitaliseringen.

Manipulering brukes mest til økonomisk svindel, eksempelvis såkalt direktørsvindel og datingsvindel, der offeret blir forledet til å utbetale penger – etter å ha blitt lurt og manipulert. Metoden brukes også til å skaffe seg informasjon gjennom spionasje. Både i direktørsvindler og industrispionasje manipuleres en medarbeider, en person på innsiden av organisasjonen, til å utføre en handling; enten det er å utbetale penger eller utlevere informasjon.

Tiltakene mot sosial manipulering er ikke så mye av teknisk art. Man må først og fremst stille seg selv noen kritiske spørsmål: Hvorfor så stort hastverk? Hvorfor skal jeg tro på denne historien, fra noen jeg faktisk ikke kjenner? Hvorfor skal de ha denne informasjonen, og hvorfor har de den ikke allerede? Hvordan kan dette være gratis? Kan dette stemme? Er det sikkert? Trygt?

Sosial manipulering (eng. social engineering): Betegnelse på metode/teknikk brukt i digital kommunikasjon for, oftest med en uvennlig hensikt, å påvirke en mottaker eller omgivelsene. Manipuleringen utnytter menneskelig kontakt og de nye møteplasser i det digitale rom, for – med dets muligheter også for skjult eller forfalsket identitet – å tilegne seg eller påvirke informasjon, og å utnytte et tillitsforhold, friste med goder eller skape frykt; i hovedsak for økonomisk vinning.
Mer: **nettvett.no/sosial-manipulering**

Bilde: Colourbox

Trendbeskrivelse

Tingenes internett

Potensiell trussel

Risiko forbundet med framveksten av det såkalte Tingenes internett (Internet of Things, kjent som IoT) begynner å bli synliggjort – og så smått erfart. Med IoT mener vi at vanlige, elektroniske gjenstander kobles på og bruker internett – både i private hjem og virksomheter. Det kan typisk være husholdningsapparater og kontorutstyr, som kjøleskap og kaffemaskin, web-kameraer og alarmer, eller også biler og roboter.

Potensialet for misbruk av kriminelle ligger særlig i at disse oppkoblede tingene brukes som en bakdør inn til andre enheter, inkl. datamaskiner og servere. Om kriminelle skaffer seg kontroll over tingene kan de brukes til andre funksjoner enn de er tiltenkt, f.eks. avlytting, tyveri av biometriske data, spredning av skadevare og spam. Kontrollen over en bil kan også overtas av hackere.

Reell risiko

Tingene som av ulike grunner er nett-tilkoblet (bl.a. for at produsentene skal skaffe seg forbrukerdata) er ofte laget med liten vekt på cybersikkerhet. De vil typisk inneholde sårbarheter som kriminelle kan utnytte, og som det i noen tilfeller er begrensede muligheter for å utbedre gjennom oppdateringer.

Trusselaktørene vil eksempelvis kunne utnytte innebygde funksjoner og sårbarheter som øyne og ører inn i et hjem eller et kontor: En smart-TV eller et sikkerhetskamera kan brukes til visuell overvåking, en babycall eller en høyttaler til avlytting. Kontroll over mange ting gjør det også mulig å knytte disse sammen i såkalte botnett (nettverk av infiserte datamaskiner), som kan brukes til annen kriminell virksomhet, inkl. tjenestenektangrep (DDoS) og spredning av skadevare.

Mulige konsekvenser

Kriminell bruk av digitale ting knyttet til internett vil kunne få store og uante følger, for privatpersoner og familier, for virksomheter og samfunnet. IoT skal i utgangspunktet lette hverdagen både hjemme og i virksomheten, men kan ved misbruk medføre det motsatte. Med IoT har trusselaktørene fått tilgang til nye sårbarheter og kan utsette ofrene for en rekke trusler og metoder som er vanskelig å oppdage for offeret.

Anbefalt aktsomhet

Forbrukere og innkjøpere bør sjekke om en vare kan kobles til nettet. Om man velger å koble enheten til et nett bør den kunne oppdateres på en enkel måte, og det er viktig å konfigurere den riktig. Til dette hører å bytte standardpassord.

Les mer: *nettvett.no/tingenes-internett/*

Tydelig trend

Trenden med at flere digitale ting kobles til internett er i rivende utvikling. IoT er et utbredt fenomen, både for privatpersoner og virksomheter. Det endrer hverdags- og arbeidsliv, mest til det bedre, men også med en ennå dårlig forstått risiko. En parallell trend, med flytende skille mellom hjem og arbeid gjør dette bare mer utfordrende.

Sikkerheten ved mange av tingene forventes å bli bedret etter hvert som IoT blir mer utbredt, og det blir stilt større krav fra forbrukerne. Samtidig vil aldri programvaren som kjører på disse enhetene bli helt fri for sårbarheter. Det betyr at det fremover må tenkes digital sikkerhet også i sammenheng med vanlige bruksgjenstander.

Global utvikling

Utviklingen av IoT skjer med enorm hastighet, og en veldig vekst. Gartner anslår at antall ting på nett vil være over 8 milliarder i 2017, med en forventet dobling i 2020. Andre opererer med noe lavere tall, uten at det endrer bildet av en eksplosiv utvikling.

Nasjonalt bilde

Utbredelsen av ting som er nett-tilknyttet er allerede stor, også i Norge; naturlig nok i et av verdens mest digitaliserte land. Anslag fra SSB viser at det trolig er over 15 millioner ting koblet til internett i Norge. NSM anslår at antallet vil tredobles fra 2016 til 2020. De som svarte på undersøkelse for Telenor i 2017 oppga at de i gjennomsnitt hadde seks påkoblede enheter. Blant annet var 35.000 sauer var koblet til nettet gjennom Telenor.

Nødvendig tiltak

Produsentene må fokusere på å utvikle sikre produkter, ikke bare for brann, stråling og lignende, men også med tanke på informasjonssikkerhet og personvern. For de som ønsker suksess i IoT-markedet vil fokus på sikkerhet være avgjørende. En type merking som viser at produktet innehar et visst nivå av sikkerhet, f.eks. at programvaren oppdateres automatisk, vil være til hjelp for distributører og innkjøpere.

Digital utpressing

Sammensatt trussel

Trusselen om utpressing er sammensatt, og rettes mot både privatpersoner og virksomheter. Mest av alt dreier det seg om økonomisk motivert utpressing. De siste årene har de kriminelles bruk av løsepenger økt drastisk. Slike angrep rettes mer og mer mot virksomheter. Private utsettes også for personutpressing, ofte med seksuelt relaterte krav. Også datingsvindel har dels karakter av utpressing, idet angriper får et emosjonelt overtak på offeret. Dette overtales, og dels trues, til å utbetale penger.

Målene for utpressingen er også sammensatt, med virksomheter av alle størrelser, individer i alle aldre. Seksualisert personutpressing rettes i stor grad både mot voksne menn og unge kvinner. Løsepengeutpressing rammer bredt, og ofte tilfeldig.

Relevant risiko

Trusselaktørene er ute etter penger, bilder eller annet materiale av verdi. Alle med informasjon på en digital enhet eller i et nettverk, løper en risiko for å bli angrepet – og presset for penger, eller også tjenester. Omfanget av løsepengevirus vokser.

Sårbarhetene som utnyttes er alt fra menneskelige følelser, tekniske sikkerhetshull i programvare, samt dårlige sikrede mobile enheter eller skykontoer.

Store konsekvenser

Utpressing kan få uante følger for den som rammes. For privatpersoner kan det ha økonomiske så vel som alvorlige psykiske og sosiale konsekvenser. For virksomheter kan det medføre dramatiske følger for både økonomi og omdømme.

Anbefalt forebygging

Utpressing kan som oftest unngås ved at man fjerner pressmiddelet. Det aller viktigste for å redusere effekten av løsepengevirus er å ha sikkerhetskopier og gode rutiner for å gjenopprette systemer ved hjelp av disse. Når det gjelder personutpressing kan det forebygges ved at man er bevisst på hvordan man lagrer intime bilder og annet, og at ikke alle er til å stole på. Gode rutiner for mobilsikkerhet. bruk av passord og totrinns verifisering på tjenester på nett vil kunne hindre informasjon i å komme på avveier i utgangspunktet.

Tydelig trend

Trenden med utpressing ved bruk av løsepengevirus er den raskest voksende cyberkriminelle aktiviteten på verdensbasis. Den har vist seg lukrativ, og tiltrekker seg organiserte og enkeltstående kriminelle, også ved at utpressingsverktøy er blitt en handelsvare. Omfanget av angrep vokste dramatisk både i 2016 og 2017, med flere typer virus, hyppigere angrep og større inntjening. Personutpressing fortsetter å være et betydelig, men lite kjent samfunnsproblem i Norge.

Metodene de kriminelle bruker utvikles basert på høstede erfaringer og blir tilpasset nye sikkerhetstiltak. Dette er særlig tilfellet for løsepengeutpressing, som er utviklet med en forretningsmodell som sikrer høy inntjening og lav risiko. Misbruk av bilder skjer til dels med nye metoder, inkl. nedlastning fra åpne kilder på nett.

Global kriminalitet

Utpressing er et globalt fenomen, og kriminelle opererer uavhengig av landegrenser. De fleste angrep rettes mot mål i en rekke land. Med betydelig betalingsevne er norske mål attraktive, og det er eksempler på kampanjer målrettet mot norske personer og virksomheter.

Nasjonalt bilde

Utpressing ved hjelp av ulike teknikker rammer mange, også i Norge, men omfanget er uklart, også fordi svært mange tilfeller ikke rapporteres eller anmeldes. I Mørketallsundersøkelsen fra 2016 ble løsepengeangrep rapportert som nest mest alvorlige hendelse av norske virksomheter. Også kommuner er blitt rammet.

Sosial manipulering

Med et av verdens høyeste datasikkerhetsnivå er det relativt få tekniske sårbarheter for de kriminelle å utnytte. Det betyr at de sannsynligvis vil fokusere på å finne nye måter å manipulere mennesker på ved bruk av frykt, tillit og fristelser – for å få flere til å trykke på en lenke eller åpne et vedlegg med skadevare som venter på å bli lastet ned.

Trendvurdering

NorSIS har identifisert to trender å følge særlig godt med på i 2018. Dette er store, dominerende globale trender i en digital tidsalder i svært rask utvikling. Trendene er relevant for både privatpersoner og virksomheter, og for hele samfunnet. Den ene, digital utpressing**, har et entydig negativt fortegn. Den andre, Tingenes internett, er overveiende positiv, men med risiko for informasjon på avveier og de konsekvenser det medfører. Begge de identifiserte trendene illustrerer digitaliseringens rivende utvikling og skyggeside.**

NorSIS følger den digitale hverdagens utvikling tett, mest av alt fra ståstedet til den enkelte databruker, og med tanke på små og mellomstore virksomheter; offentlige og private. Tingenes internett (IoT) har ikke rukket å bli et dagligdags begrep, men fenomenet tilhører hverdagens realiteter. Det endrer dagligliv og arbeidsliv på en mer gjennomgripende måte enn vi kanskje evner å se.

NorSIS har valgt Tingenes internett som én trend som er verdt særlig oppmerksomhet. Den angår alle, og skal hjelpe oss der vi er: hjemme og på arbeid. Samtidig som det kan bidra til et sikrere samfunn, representerer IoT en trussel for en sikker digital hverdag! Dernest er digital utpressing valgt, også det på grunn av store konsekvenser, både for enkeltpersoner og virksomheter – og som samfunnsproblem. Utpressing inkluderer flere trusler, som personutpressing og løsepengevirus.

Tingenes internett er her

IoT er for noen allerede en del av hverdagen og vil fremover bli en enda større del. Ofte vil slik teknologi fungere uten at vi som forbrukere eller ansatte tenker over hva som skjer. Sensorer i for eksempel veidekke, vil kunne øke trafikksikkerheten. Sensorer og datakapasitet i en bil som andre overtar kontrollen av, vil svekke trafikksikkerheten. Dagens bil er i bunn og grunn en rullende datamaskin.

Det vil gjøre møter effektive med bedre hjelpemidler og tilgjengelighet – og overvåke dem gjennom en kaffemaskin som lytter og en prosjektor som ser. Her er rom for kreative skrekkscenarioer, hvor IoT gir Internett, og de kriminelle, øyne og ører. Med roboter får de også armer og bein - og kunstig intelligens. IoT kan også åpne for utpressing, selv i det små. Som når cybersmåkriminelle har tatt over kaffemaskinen, og forlanger femti kroner for tilgang. Uintelligent, men kanskje effektivt.

«Et typisk eksempel på «sextorsion» er at man har snakket over Skype, hvor den ene parten tilbyr å kle av seg mot at den andre gjør det samme. Det offeret ikke vet er at samtalen tas opp og brukes som pressmiddel for penger».

Slettmeg.no

Digital utpressing er her for fullt

NorSIS legger flere trusler og metoder i kategorien utpressing. Flere sikkerhetsaktører framholder løsepengevirus som den aller største digitale trussel på global basis. Dette var i 2017 konklusjonen også til Europol. Nasjonal sikkerhetsmyndighet forventer at utpressingskampanjer med løsepengevirus i enda større grad vil treffe også Norge. Årsaken er åpenbar: Metodene er enkle, angrepene billige, gevinstene store – mens risikoen er minimal.

Europol kaller spredningen av løsepengevirus en epidemi. «WannaCry» bidro i 2017 sterkt, ved å ramme rundt 400.000 maskiner i over 150 land. Norge ble truffet, men lite rammet. Det illustrerer at virus ikke lett finner sårbarheter i land med så høyt sikkerhetsnivå som Norge, og at angriperne er avhengig av at noen åpner og aktiverer skadevaren. Nye virus og angrepsmåter ventes, også mer mot mobile plattformer.

Omfanget forventes økt også fordi teknologien er enkel å bruke – og er til salgs. Det ventes økning i omsetning av slike «ransomware-as-a-service»-tjenester (RaaS) på det mørke internettet. Hvem som helst kan bli en virusspreder og cyberutpresser. E-post er i dag den mest vanlige metoden for å spre løsepengevirus. Bevissthet om faren ved å åpne vedlegg og aktivere lenker er dermed den beste forebygging. Så vil de kriminelle ventelig finne nye måter – og nye veier.

Ved personutpressing brukes sensitiv, ofte intim, informasjon til utpressing. Særlig utsatt er de med nakenbilder på avveier, som blir brukt til å presse dem for enda flere bilder, til seksuelle handlinger – og for penger. NorSIS har lenge fulgt denne delen av trusselbildet tett gjennom tjenesten Slettmeg.no. Det er en relativ stabil trussel, med kjente metoder. Omfanget er ikke svært stort, men det har store konsekvenser for de som rammes. NorSIS anser derfor denne type krenkelser som et samfunnsproblem, også fordi det utfordrer rettssikkerheten. Dette inkluderer en tendens i retning av at navn på folk som krenker andre, eksempelvis de som deler bilder uten samtykke, blir offentliggjort. Delingen er ulovlig; dét er også selvtekt.

«Selv om du ikke er på nett med annet enn en mobiltelefon, er du en del av Tingenes internett. Det er ikke et separat internett, men det samme vi bruker hver dag med mobilen eller PC-en. På den måten har Tingenes internett en påvirkning på oss alle».

Nettvett.no

Bilder på nettet trenger ikke være stjålet for å bli brukt til utpressing. En tendens er at de blir funnet på nettet, hvoretter den kriminelle finner – og kartlegger – personen, eksempelvis ved bildegjenkjenning i Google. Så presses vedkommende for penger, under trussel om spredning. Mye tyder på at det også her er internasjonale kriminelle som står bak. Enkeltvis er det små saker med små summer som går under radaren; i realiteten også hos Politiet, som i liten grad er skodd for å gå etter denne typen kriminalitet.

Trussel om offentliggjøring er også en tendens i løsepengevirusangrep. Fra å låse og eventuelt ødelegge data, truer kriminelle med å offentliggjøre dem. En annen kjent teknikk bruk til utpressing er tjenestenektangrep (DDoS): Hvis det ikke betales, stenges tjenesten. Kriminelle går etter verdiene der de finnes. De bedriver innovasjon, søker nye mål og nye markeder.

Bilde: Colourbox

Verdier å beskytte, verdikjeder å sikre

Digitale verdier kan være så mangt, og de fleste har noen. Digitale verdikjeder er vanlige i stadig mer komplekse leveranser og en globalisert verden.

Den datakriminelle aktiviteten er global og metodene er universelle. Kriminelle går etter verdier der de måtte finnes, enten de befinner seg i den digitale verden eller nås via digitale nett. Verdier søkes og sårbarheter identifiseres, før angrep settes inn.

Verdifull informasjon er et typisk mål, enten den har verdi i seg selv, eller som middel for å komme til andre verdier. Til denne typen hører typisk passord og personopplysninger, som kan brukes både til informasjons- og ID-tyveri. Intellektuell eiendom og sensitiv informasjon kan ha kritisk forretningsverdi for en virksomhet, og kan komme på avveier også gjennom spionasje. Verdier kan også angripes og ødelegges gjennom sabotasje. For en privatperson kan digitale dokumenter, som foto, ha stor affeksjonsverdi. Slike, og andre (intime) bilder, så vel som annen informasjon på avveier, kan ha verdi som utpressingsobjekt.

Verdier finnes også i verdi- og leveransekjeder. Komplekse løsninger krever ofte at flere aktører bidrar til en leveranse. Mange mindre virksomheter er med som underleverandører, og de kan være et mer attraktivt angrepsmål enn en stor hovedleverandør – som ofte har bedre systemer for informasjonssikring. Mindre bedrifter kan selv ha verdier som vekker kriminell interesse – eller de kan være en ubevoktet vei inn til andre. Verdikjeder øker eksponeringsflaten, og kan øke risikoen. Det samme kan være tilfellet med tjenesteutsetting («outsourcing») til en tredjepart. Det gjelder særlig hvis denne har dårlig sikkerhet, eller også når eier av informasjonen selv har for dårlig kontroll over sine verdier.

Tiltak for å sikre verdiene fordrer bevissthet: Først om hvilke verdier som faktisk finnes, dernest hvilke sårbarheter som skaper risiko for å miste dem. Da må både en verdikartlegging og en risikovurdering gjennomføres – før sikkerhetstiltak velges. Grunnleggende verdiforståelse er vesentlig både for den som angriper og den som skal sikre. Verdiene inkluderer virksomhetens informasjon og eiendeler (digitale og fysiske), men også kompetanse, dvs. også mennesker.

Truslene er langt på vei universelle og ganske statiske; metodene er mye mer dynamiske. Hvilke trusler som er mest overhengende avhenger av verdiene som finnes – og hvilken verdi de har for hvem. Lokale trusselvurderinger og lokale risikovurderinger må legges til grunn for valg av sikringstiltak, både i et hjem og i en virksomhet. Trusselbildets logikk er enkel: Verdier tiltrekker seg trusler; trusselaktører utnytter sårbarheter; sårbarheter eksponerer verdiene – som så (kanskje) angripes.

Sikring av verdier starter derfor med enkle spørsmål: Hvilke verdier finnes? Hvilke trusselaktører er sannsynlige? Hvilke sårbarheter kan de utnytte? Hvilke mottiltak kan treffes? Noen svar, noen tiltak, er universelle; andre er spesifikke. Grunnleggende tiltak – uten unntak – innbefatter de tre k-ene: kartlegging, kunnskap, kultur. Menneskelig kompetanse og organisatorisk orden – virksomhetens kultur og struktur – må gå hånd i hånd med grunnleggende teknologiske tiltak.

Risikovurderinger vil bidra til å gjøre virksomheten klar over hvilke utfordringer man står overfor. I tillegg gir risikovurderinger grunnlag for å beslutte hvilke tiltak som bør iverksettes. Man unngår mer eller mindre tilfeldige tiltak som mangler faglig fundament og risikerer å bli prioritert bort.
NSM «Risiko 2017 Risiko og Sårbarheter i en ny tid».

TILLEGG

2017–18

Tilnærming til trygghet

Sikkerhet er en forutsetning for trygghet. Det gjelder også i det digitale området. NorSIS har som samfunnsoppdrag å bidra til en trygg digital hverdag – for alle. Digital trygghet fordrer en mest mulig sikker bruk av verktøy og nettverk, med minst mulig sårbarhet, og en så lav risiko som realistisk mulig for digitale angrep: Trusler om nettbaserte innbrudd, overfall og ran. Sikkerhet forutsetter sikre systemer, men også bevisste enkeltpersoner med sikker atferd.

NorSIS skal bidra til digital trygghet – for alle i Norge. Med «alle» menes i prinsippet alle brukere av digitale enheter og tjenester; alle landets databrukere: Rundt regnet fem millioner individer. De er i utgangspunktet enkeltpersoner; privatpersoner. Dernest er de fleste også elever og studenter, ansatte og eiere – i en offentlig eller privat virksomhet.

Dette er hovedtilnærmingen til NorSIS: Se på individet som en nøkkel til sikkerhet, mer enn som en sikkerhetstrussel. De er i utgangspunktet ikke svake ledd i en sikkerhetskjede, men helt essensielle sikkerhetsforsvarere. Men de kan blir svake ledd hvis de ikke er tilstrekkelig bevisste, med en ansvarlig atferd. Og da trengs kunnskap og kompetanse om trusler og tiltak hos den enkelte – og kultur for informasjonssikkerhet i virksomheter.

NorSIS i samfunnet

NorSIS er en frittstående, uavhengig organisasjon, uten kommersielle eller politiske bindinger. Samfunnsrollen er å bruke spisskompetansen til å spre kunnskap, bidra til bevisstgjøring og beskyttelse mot digitale trusler, ikke minst ved å fremme en kultur for informasjonssikkerhet i det norske samfunnet – i hverdagen.

Individet i sentrum

Sikkerhetsfaget opererer klassisk med tre typer faktorer i risikovurdering og sikringstiltak: teknologiske, organisatoriske og menneskelige. Mange har, helt nødvendig og naturlig, sitt hovedfokus på den første og andre dimensjonen. Det gjelder eksempelvis for den viktige veilederen «Grunnprinsipper for IKT-sikkerhet» fra Nasjonal sikkerhetsmyndighet (NSM). Den omhandler teknologiske og organisatoriske tiltak, men vil senere suppleres med også det menneskelige perspektivet. NorSIS inkluderer alle, men har lagt sin hovedvekt mot den siste delen – med mennesket og dets rolle i organisasjonen, og med individet i sentrum.

NorSIS er opptatt av at sikkerhetsfokuset må være like mye på mennesker som på maskiner; på kultur som på struktur; på vanvare som på skadevare. NorSIS har sine hovedmålgrupper oppsummert; enkeltpersoner og virksomheter. Til den første gruppen tilhører alle databrukere, enten som privatpersoner eller ansatte; til den siste: særlig små og mellomstore bedrifter samt kommuner.

Bilde: Maria Nyheim

Kronologi 2017

Sammenstillingen innbefatter et utvalg digitale hendelser i eller med relevans for Norge og norske databrukere i 2017. Oversikten er hentet fra media og er todelt; med trusler og tiltak.

Trusler og angrep

JANUAR
NorSIS gjør oppmerksom på at appen Discord brukes til deling av nakenbilder av norske jenter, og publiserer en veiledning for sletting.

TV2 omtaler Politiets innbyggerundersøkelse 2016, som viser at 7 % av de spurte er blitt utsatt for nettsvindel; mer enn noen annen type kriminalitet.

FEBRUAR
NorSIS offentliggjør en ny kartlegging av ID-tyveri gjennomført med Skatteetaten, som viser at 4,2 % av den voksne befolkningen er rammet.

DSB offentliggjør sin befolkningsundersøkelse, der 30 % av de spurte uttrykker bekymring for at cyberangrep skal ramme samfunnssikkerheten.

Telenor advarer om en ny bølge løsepengevirus gjennom e-post som utgis for å være en faktura, og NorSIS advarer mot å åpne vedlegg.

NRK avslører at utenlandske underleverandører til det norske selskapet Broadnet, uten norsk sikkerhetsklarering, har hatt tilgang til deler av Nødnett.

Media melder at det er avdekket at detaljerte kundedata fra Æ-appen lå åpent tilgjengelig i to uker før sikkerhetshullet ble tettet, og Rema korrigerer.

VG melder at e-post-adresser og passord til et betydelig antall norske politikere, departements- og ambassadeansatte er på avveie etter hacking.

NorSIS opplyser om at data fra en CloudPets-leke har vært åpent tilgjengelig, og bruker-/persondata om et stort antall barn kan være på avveie.

MARS
NorSIS advarer mot å klikke på en lenke i en e-post mange har mottatt, tilsynelatende sendt fra en .no-adresse, med krav om løsepenger.

Digi.no melder at feil i Amazons skybaserte lagringstjeneste S3 har rammet selskapet selv og mange tusen andre nettsteder og -tjenester.

NSM advarer mot krypteringsviruset TorrentLocker, rettet mot private og bedrifter, som låser innhold på PC-er, med krav om løsepenger for å frigi filene.

Skatteetaten advarer mot et svindelforsøk (phising), der mottakerne forsøkes fralurt sin BankID gjennom falske e-poster som utgir seg for å være fra etaten.

NRK avslører at utenlandske underleverandører til selskapet Sykehuspartner har hatt tilgang til nordmenns helsedata etter outsourcing fra Helse Sør-Øst.

NRK melder at en kompromittert tredjepartstjeneste har ført til at tusenvis at Twitter-kontoer, også norske, er misbrukt til å sende ut tyrkisk propaganda.

APRIL
DNB advarer mot et svindelforsøk ved bruk av SMS (smishing) der falske meldinger, med selskapet som avsender, dels la seg i samme tråd som ekte.

Dinside.no skriver at nordmenn i 2016 ble svindlet for 137 millioner kroner etter å ha blitt frastjålet kortinformasjon på internett, bl.a. fra falske nettbutikker.

MAI
Skadevaren WannaCry sprer seg uvanlig raskt til over 150 land, også Norge, gjennom en sårbarhet i Microsofts fildelingsprotokoll.

Skatteetaten advarer mot et nytt svindelforsøk med falske e-poster som ber om persondata-informasjon, fordekt som en melding om skatterefusjon.

SSB offentliggjør statistikk som viser at 56 % av statlige virksomheter opplevde forsøk på ID-tyveri i 2017, som den alvorligste sikkerhetstrusselen.

Næringslivets Sikkerhetsråd slår alarm om mangelfull sikkerhetsbevissthet hos næringslivsaktører etter et større norsk delegasjonsbesøk til Kina.

Datatilsynet minner om at moderne biler lagrer og behandler store mengder data, også personopplysninger, som brukeren må være kjent med og akseptere.

JUNI
NorSIS melder at flere privatpersoner og virksomheter har mottatt svindel-e-post med trussel om DDoS-angrep hvis de ikke betaler 1 bitcoin (da ca. 25.000 kroner).

NorSIS melder at Kaspersky Lab har avdekket trojaner-skadevare på apper i Google Play, og anbefaler å være kritisk til ukjente apper, hvorav flere falske.

NSM opplyser at to flernasjonale konsern med selskaper i Norge, Optimera og Møller-Mærsk, er rammet i et nytt globalt løsepengevirus-angrep.

VG melder at norske soldater fra Telemark bataljon utsettes for russisk hybridangrep, i form av falske rykter og påstander under NATO-tjeneste i Litauen.

AUGUST
VG skriver om spredning av et virus på Facebook som oppretter meldinger som så sendes venner, med den antatte hensikt å samle personinformasjon for salg.

NorSIS melder at sikkerhetsselskapet Lookout har oppdaget en sårbarhet i over 500 apper i Google Play, der spionvare kunne installeres på brukerens mobiltelefon.

NorCERT informerer om en løsepengevirus-kampanje under spredning som minner om WannaCry, og som vil låse innholdet på datamaskinen.

NorSIS advarer mot en pågående nettsvindel med spredning av falske konkurranser via e-post og sosiale medier, hvor bl.a. SAS er misbrukt.

Digi.no skriver om appen «Trygg på reise» fra Tryg, som har åpnet for tapping av data om norske kjøretøy så vel som deres eiere.

NorSIS uttaler seg kritisk til den populære appen Sarahah, som kan brukes – og blir brukt – til nettmobbing.

SEPTEMBER
E-tjenestens sjef advarer mot utstrakt bruk av sosiale medier, og ser det som problematisk at store kommersielle selskaper sitter på mye persondata.

NSM forventer i «Helhetlig IKT-risikobilde 2017» økning i målrettet spredning av skadevare via e-post til privatpersoner, og fortsatt bruk av løsepengevirus.

NorCERT informerer om flere sårbarheter i Bluetooth-protokollen som gjør det mulig for angripere å installere skadevare og stjele innloggingsdetaljer.

NorSIS melder at hackere har spredd skadelig botnett-programvare via en oppdatering av programmet CCleaner, fra en kompromittert nedlastingsserver.

OKTOBER
NorSIS melder om et påvist sikkerhetshull i WiFi-protokollen WPA2; en sårbarhet som åpner for tyvlytting og modifisering av trafikk mellom aksesspunkt og klient.

NRK avslører på ny at en utenlandsk underleverandør til selskapet Sykehuspartner har hatt uautorisert tilgang til sensitive helsedata fra Helse Sør-Øst.

NOVEMBER
NRK melder at svindlere forsøker å lure til seg Netflix-brukeres betalingsinformasjon gjennom falske e-poster, ved å true med å sperre kontoen.

Håndballstjernen Nora Mørk forteller at hennes private bilder er spredd på internett etter hacking via en app, og at hun vil anmelde de som har spredd dem.

Trondheim kommune stenger appene Saraha og Polly grunnet funn fra sine nettverk etter at de er brukt til mobbing, hatmeldinger og krenkelser blant skoleelever.

Bransjeorganisasjonen Virke advarer mot direktørsvindel, etter et oppsving av meldinger om slike svindelforsøk, mot både større og mellomstore bedrifter.

NorSIS advarer mot et svindelforsøk ved hjelp av en e-post som utgir seg for å komme fra Netflix, med forsøk på å lure til seg betalingsinformasjon.

NorSIS informerer om mottatte meldinger om forsøk på såkalt direktørsvindel rettet også mot norske kommuner, omtalt som «rådmannssvindel».

VG melder at om en avansert cyberspionasje-operasjon fra en utenlandsk etterretningsaktør, rettet mot Norsk utenrikspolitisk institutt.

Tiltak og rapporter

JANUAR
KPMG offentliggjør en ny global undersøkelse som viser at forbrukere bør være mer bevisste på hvilke personopplysninger de oppgir ved netthandel.

NorSIS avholder for sjuende gang den årlige Security Divas-konferansen for å samle og inspirere kvinner med interesse for informasjonssikkerhet og IKT.

FEBRURAR
NorSIS avholder, sammen med Politidirektoratet og Skatteetaten, den årlige Identitet-konferansen, med fokus på identitet og ID-forvaltning, og sikker samhandling som hovedtema.

MARS
NSM legger fram rapporten «Risiko 2017» og understreker at selv om Norge er et trygt land, må vi – for å beskytte verdiene våre – redusere sårbarhetene.

APRIL
BDO legger fram sin årlige Risikoundersøkelse blant 1500 norske ledere i privat og offentlig sektor, som rangerer dataangrep som den fremste trusselen.

Kripos advarer mot stor økning i stadig mer avansert datakriminalitet, og oppfordrer både privatpersoner og bedrifter til å anmelde slike hendelser.

MAI
CLTRe publiserer en ny rapport om informasjonssikkerhetskultur, med data fra Norge og Sverige, som bl.a. peker på kjønn, alder og ansiennitet som faktorer.

JUNI
Justis- og beredskapsdepartementet legJustis- og beredskapsdepartementet legger fram Stortingsmelding nr. 38, «IKT-sikkerhet – et felles ansvar», som redegjørelse om regjeringens politikk på området.

Forsvaret legger fram sin årlige innbyggerundersøkelse, der trusselen om et cyberangrep på Norge skårer høyest, foran kriminalitet og terror.

KMPG legger fram sin «Cyber Security Benchmark 2017» som viser at hele 72 % av de norske selskapene ikke har med cybersikkerhet i sine årsrapporter.

NSM melder at BDO, gjennom BDO CERT, blir det første norske selskapet som tilfredsstiller kravene i dets kvalitetsordning for digital hendelseshåndtering.

JULI
KPMGs lederundersøkelse viser at hver tredje norske IT-topplеder mener deres selskap har god nok cyberberedskap, og flest er bekymret for organisert kriminalitet.

IKT–Norge peker på at Sveriges erfaring med at bortsetting av tjenester gir uvedkommende tilgang til sensitive offentlige data må føre til bedre sikring også i Norge.

AUGUST
NorSIS legger fram undersøkelsen om ungdom og digital sikkerhetskultur, som viser at bare 7 % av ungdommen får opplæring i informasjonssikkerhet.

Telenor presenterer sin sikkerhetsrapport og melder om en registrert økning av kriminelle svindelforsøk rettet mot norske selskaper og ledere (CEO-svindel).

NSM publiserer en revidert versjon av sin publikasjon «Grunnprinsipper for IKT-sikkerhet», om hva en virksomhet bør gjøre for å sikre et IKT-system, og hvorfor.

Regjeringen legger fram «Internasjonal cyberstrategi for Norge» som bidrag til forebygging av og beskyttelse mot trusler mot Norge og norske interesser.

Justis- og beredskapsdepartementet offentliggjør en rapport som påviser framtidig økt behov for IKT-sikkerhetskompetanse, som bidrag til en ny strategi på feltet.

SEPTEMBER
Regjeringen nedsetter et utvalg for å se på regelverk og organisering innen IKT-sikkerhet, som oppfølging av Stortingsmelding nr. 38.

NorSIS tildeler Fiduspрisen 2017 til Coop Norge Handel AS for selskapets fokus på sikkerhetsarbeid og forankringen av dette i virksomhetens øverste ledelse.

Forbrukerrådet publiserer en rapport som påviser personvernmangler ved bruk av app-tilkoblede blodtrykks- og blodsukkermålere.

SSB offentliggjør statistikk som viser at 90 % av nordmenn mellom 16 og 79 år bruker internett daglig; to av tre bruker sosiale medier daglig.

NSM lanserer, i samarbeid med flere aktører, et opplæringsprogram for bedrifters ansatte for bedre å håndtere sårbarheter knyttet til Tingenes internett (IoT).

OKTOBER
NorSIS står bak den årlige Nasjonal sikkerhetsmåned; en dugnad med deltakelse fra en lang rekke offentlige og private aktører.

Nkom og NSM legger fram en undersøkelse blant bedrifter på Sørlandet, som viser økt bevissthet om informasjonssikkerhet sammenlignet med året før.

Forbrukerrådet legger fram en rapport om sikkerhetsbrister ved GPS-klokken Gator for barn, som via en app kan tas kontroll over, med sporing og avlytting.

NOVEMBER
NorSIS presenterer sin tredje rapport om informasjonssikkerhetskultur i Norge – «Nordmenn og digital sikkerhetskultur 2017» – som bl.a. etterlyser mer kunnskap.

PWC legger fram sin «Cybercrime Survey 2017» med danske og norske tall, som viser at organisert kriminalitet og ansattes ubevisste handlinger anses som største trusler.

Politiforum melder at politidirektøren garanterer for at arbeidet med å etablere et nasjonalt cybercrime-senter, et NC3, vil starte for fullt i 2018.

Barn og medier offentliggjør en undersøkelse som viser at 15 % av jenter i alderen 13–16 år har sendt nakenbilder; 26 % av dem har følt seg presset til det.

Høgskolen i Innlandet (HINN) kunngjør at det, i samarbeid med Datatilsynet, vil innføre et emne i personvern i 2018, etter at EUs personvernforordning skjerper kravene.

DESEMBER
Stortinget vedtar gjennom statsbudsjettet for 2018, for første gang, å bidra til finansieringen av veiledningstjenesten Slettmeg.

Referanser 2017

«Trusler og trender 2017–18» er en kvalifisert utvelgelse av de ti fremste cybertruslene rettet mot privatpersoner og virksomheter i Norge i 2017, inklusive to av de rådende trendene på informasjonssikkerhetsområdet i 2017–18. Rapporten er resultat av systematisk vurdering, med referanse til nasjonale og internasjonale kilder, så vel som erfaringsbasen til NorSIS

Det nasjonale bildet

NorSIS bygger denne rapporten i utstrakt grad på egne erfaringer over flere år, og tett kontakt med norske nettbrukere. Dette gjelder særlig privatpersoner og mindre virksomheter. I tillegg har NorSIS nær faglig kontakt med en rekke sentrale aktører på feltet, både offentlige, private og frivillige.

Det er begrenset systematisert kunnskap om informasjonssikkerhet i Norge. En del av det som finnes er skaffet til veie gjennom undersøkelser utført av NorSIS, inklusive (i 2017) «*Ungdom og digital sikkerhetskultur*» og «*Nordmenn og digital sikkerhetskultur*». NorSIS utfører også en årlig undersøkelse om ID-tyveri sammen med Skatteetaten. Telenor utga rapporten «*Digital Sikkerhet 2017*» som også favner bredt, basert på selskapets erfaring med en stor del av data-trafikken i Norge.

Enkelte sikkerhetsselskaper har gjennomført undersøkelser og publisert rapporter med data fra privat sektor. Til disse hører (i 2017) «*Risikoundersøkelsen*» fra BDO, «*Cybercrime Survey 2017*» fra PwC og «*Lederundersøkelsen 2017*» fra KPMG. «*Mørketallsundersøkelsen*» fra Næringslivets Sikkerhetsråd (NSR), som NorSIS deltar i arbeidet med, kommer ut annethvert år, sist i 2016. NSR står også bak «*Kriminalitets- og sikkerhetsundersøkelsen i Norge 2017*». Det norske selskapet Mnemonic utgir en årlig sikkerhetsrapport, «*Security Report 2017*», som har et internasjonalt nedslagsfelt.

På overordnet statsnivå utgir E-tjenesten og Politiets sikkerhetstjeneste (PST) årlige åpne trusselvurderinger der cyberdomenet er med. Det samme gjør Nasjonal sikkerhetsmyndighet (NSM), både med «*Risiko 2017*» og mer spesifikt for informasjonssikkerhet med «*Helhetlig IKT-risikobilde 2017*». Særlig den siste er en grundig vurdering på flere nivåer og med flere aspekter.

«*Trusler og trender 2017–18*» bygger også på disse og andre norske kilder.

Det internasjonale bildet

Det digitale trusselbildet er i all hovedsak globalt. Datakriminaliteten er internasjonal, de fleste utviklingstrekk – med nye metoder så vel som trender – er globale. De vil derfor i avgjørende grad prege også norsk digital hverdag. NorSIS følger denne utviklingen, og relaterer den til norsk virkelighet.

Det er omfattende informasjon om og vurderinger av trusler og trender fra det internasjonale cybersikkerhetsmiljøet, fra både offentlige og private kilder. Til de siste hører særlige store rådgivingsselskaper, som – ut fra sin forretningsvirksomhet – har noe forskjellige tilnærminger og konklusjoner. På en rekke områder avtegnes likevel et noenlunde ensartet trusselbilde, som også reflekteres i dette dokumentet. Det gjelder typisk utvikling av løsepengevirus som en global hovedtrussel.

En rekke selskaper utgir trusselrapporter. Blant de mange NorSIS har gjennomgått i arbeidet med dette dokumentet er: «*2017 Security Cyber Threatscape Report*» (Accenture); «*Top Security Threats 2017*» (Calyptix); «*Trends in Cybersecurity 2016/17*» (CapGemini); «*2017 Annual Cybersecurity Report*» (Cisco); «*2017 Cyberthreat Defence Report*» (CyberEdge Group); «*Kaspersky Lab Threat Predictions for 2018*» (Kaspersky); «*2017 Threat Predictions*» (McAfee/Intel); «*Security Intelligence Report*» (Microsoft); «*Internet Security Threat Report*» (Symantec); «*2017 Data Breach Investigations Report*» (Verizon).

Fra flernasjonalt, offentlig hold er bl.a. disse rapportene brukt: «*Threat Landscape Report 2016*» (Enisa) og «*2017 Internet Organised Crime Threat Assessment*» (Europol).

«*Trusler og trender 2017–18*» bygger også på disse og andre internasjonale kilder.

Trusler og trender 2017–18 er en del av kjernevirksomheten til NorSIS; et ledd i å fremme kunnskap rundt og bevissthet om digitale sårbarheter og trusler, som et bidrag til å skape en trygg digital hverdag.

NorSIS er en uavhengig organisasjon som arbeider for å styrke norsk informasjonssikkerhet, med hovedvekt på å bevisstgjøre og bistå enkeltindivider og mindre virksomheter, både private og offentlige. Disse er blant de mest sårbare, særlig for den tiltagende nettkriminaliteten, fordi de i utangspunktet har færre ressurser å sette inn for å beskytte seg. Bevissthet om hvilke verdier som står på spill, og hvor en er særlig sårbar for angrep, er det beste utgangspunkt for å treffe forebyggende tiltak.

NorSIS arbeider bredt for å spre kunnskap, skape bevisshet og gi veiledning. Blant våre viktigste tiltak og tilbud er disse:

Nasjonal sikkerhetsmåned er en nasjonal dugnad med bred deltakelse, med vekt på informasjon og opplæring. NorSIS er nasjonal tilrettelegger og koordinator av Sikkerhetsmåneden, som arrangeres hvert år i oktober.
www.sikkert.no

Nettvett er en nasjonal veiledningstjeneste, med grunnleggende råd om styrket sikkerhet og oppdatert rettledning om håndtering av trusler. NorSIS er redaktør av Nettvett, som drives i et samarbeid med NSM og NKOM.
www.nettvett.no

Slettmeg er en nasjonal veiledningstjeneste, med grunnleggende råd og personlig veiledning for de som opplever krenkelser på nett. NorSIS har utviklet og bemanner Slettmeg, som består både av et nettsted og en rådgivingstjeneste.
www.slettmeg.no

www.norsis.no

NorSIS
Norsk senter for informasjonssikring

Trusler og trender 2017–18 er utgitt av NorSIS

BDO

Trusler og trender 2017–18 er støttet av BDO

Bilde: Maria Nyheim