Trusler og trender 2015

NorSIS

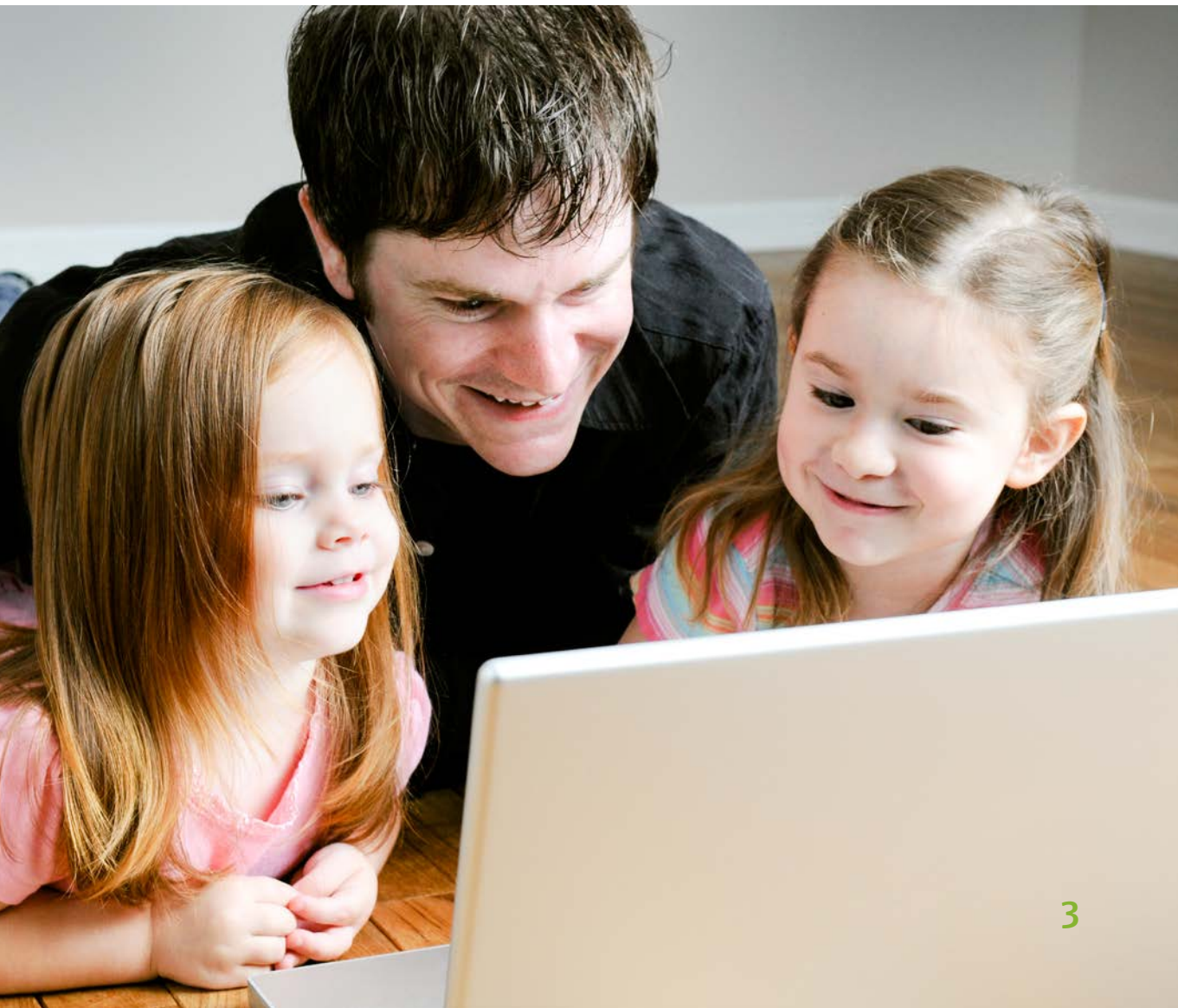
Norsk senter for informasjonssikring

Innledning

Vår hverdag har i løpet av bare noen få år blitt radikalt forandret. 95 % av norske husstander var i 2014 på nett. Leverandører av varer og tjenester har omfavnet den digitale utviklingen. I dag kan man få kroppsnær teknologi som gir beskjed når man skal opp fra sofaen og vaskemaskiner som kan overvåkes via en app på mobilen. De tekniske apparatene generer mye informasjon om våre forbruksvaner. I tillegg benytter vi som personer sosiale medier til å utveksle enda mer informasjon. Internett gir oss uante muligheter, bidrar til verdiskaping og åpner nye sosiale arenaer. Summen av all informasjon om hver enkelt kan derimot utnyttes av kriminelle. Datakriminalitet gir høy gevinst og de kriminelle har lav risiko for å bli tatt.

Virksomheter har store muligheter for gevinstrealisering ved bruk av digital teknologi. Geografisk lokasjon er ikke relevant så lenge man har digitale skytjenester og felles portaler. Fordelene kan imidlertid utnyttes av kriminelle og målrettede angrep utføres mot virksomheter for å få tilgang til verdifull informasjon.

Foto: iStockphoto



Direktørens ord

Cybertrusselen er i endring

IKT gjennomsyrer hele samfunnet og har blitt fundamentet for verdiskaping og vår felles velferd. I takt med digitaliseringen av samfunnet, så følger kriminaliteten etter. Internett har også blitt en arena for konflikt og kriminalitet. De senere tids hendelser indikerer:

1. Krenkelser på nett: Vi ser en økende tendens til anonym mobbing og publisering av bilder uten tillatelse på nett. Unge mennesker får livene sine ødelagt og plageåndene går fri. På Facebook, Twitter og Instagram er det etablert egne arenaer hvor formålet kun er å spre rykter og usanne påstander. Fenomenet sprer seg fra høyskoler og universitet til barneskoler. Trenden er at jenter oftest er ofrene, men samtidig er det de som står for mest krenkende kommentarer.

Roger Johnsen, administrerende direktør i NorSIS

2. Kriminaliteten flytter seg til internett: Det foreligger indikasjoner på at kriminelle i økende grad velger å nyttiggjøre seg cyberteknikker. Identitetstyveri, svindel og tyveri er utbredte former for datakriminalitet, men også svært alvorlig kriminalitet som barnepornografi, omsetting av narkotika og utpressing har funnet nye former på internett. Underrapportering og tilbakeholdenhet med å anmelde datakriminalitet virker å være en trend.

3. Ekstremister bruker internett til å nå sine mål: Tidligere har ekstremister i hovedsak anvendt internett til rekruttering og spre sitt budskap. Enkelte slike grupperinger virker nå å ha tilegnet seg nødvendig kunnskap til også å kunne gjennomføre cybersabotasje og forårsake forstyrrelser på internett. Viljen er nok foreløpig større enn evnen. Vi kan derfor anta at de vil velge seg lett tilgjengelige og sårbare virksomheter som mål for sine angrep.

4. Fremmede makter gjennomfører cyber-etterretning i Norge: Stater med kapasitet til å utplassere utstyr og analysere store datamengder lykkes i å gjennomføre slike operasjoner uten at de blir avslørt. Overvåking av mobilnettet er bare en av flere cyberteknikker som anvendes. Spionasje via internett er trolig enda mer utbredt.

De senere år har det blitt utført en rekke terrorhandlinger mot sårbare grupper, tilfeldige ofre og lettere tilgjengelige mål. Etter angrepene på Charlie Hebdo, så oppgir det franske forsvarsdepartementet at ekstremister har igangsatt omfattende cyberangrep som rammer lett tilgjengelige mål som skoler, kirker, mindre bedrifter og offentlige institusjoner. Nærmere 90 % av norske virksomheter tilhører denne kategorien og ligger utenfor den beskyttelse myndighetene har etablert for kritisk infrastruktur.

Små virksomheter, kommuner og enkeltmennesker kan bli rammet av avansert cyberkriminalitet og ekstremistisk motiverte hackerangrep. Samarbeid mellom myndighetene, norske virksomheter og cybersikkerhetsbransjen er viktigere enn noen gang. Ikke bare når det gjelder å finne en hensiktsmessig organisering og rollefordeling, men kanskje aller viktigst hvordan vi skal sørge for utdanning av personell som kan forebygge og bekjempe cyberkriminalitet. NorSIS arbeider for at alle skal kunne bruke internett og IKT trygt på jobb og privat.

Foto: iStockphoto.com

Ny digital hverdag

Vår digitale hverdag har de siste årene blitt kraftig forandret. Jobb, sivilstatus og forbruksmønster er retningsgivende for hvilket digitalt liv vi fører. For bare noen få år siden var PC et verktøy vi benyttet til tekstbehandling og utveksling av e-post. I dag er vi nærmest kontinuerlig på nett, via alt fra mobiltelefoner, nettbrett, PC-er, TV-er, vaskemaskiner til biler. Ny jobb, kjærester og venner finner man på internett. Hverdagen har endret seg drastisk.

Den digitale arena gir store muligheter for sosialt samkvem uten hensyn til geografisk avstand. Tidligere studiekamerater, venner og familie spredt over hele verden forenes digitalt i våre liv. Offentliggjøring av bilder og personlig informasjon gir imidlertid nettplagere en anonym arena for krenkende kommentarer. Vi ser at private intime bilder publiseres i hevnaksjoner fra tidligere kjærester eller venner.

Fysisk sikkerhet er en del av hverdagen vår, enten det er å feste sikkerhetsbeltet når man kjører bil, eller sikre båten eller campingvogna når værvarselet melder høststorm. I en arbeidssituasjon er fysisk sikkerhet knyttet til å unngå skader, og å beskytte liv og helse, såkalte HMS-tiltak. Alle disse nevnte tiltak gjennomfører man før hendelser inntreffer.

I vår digitale verden er det ikke like lett å forutse hendelser slik at man kan ta de rette forholdsregler for å beskytte seg. Og hva skal man beskytte? Digitale verdier er alt fra saksdokumenter og bedriftshemmeligheter til våre private bilder og personlig informasjon. Antivirus installeres for å forhindre angrep som kan medføre tap og ødeleggelse av informasjon. En sikkerhetskopi reduserer risiko for tap av informasjon hvis en hendelse inntreffer. Likeledes konfigurering av en brannmur, hvem skal vi slippe

Foto: Guian Bolisay

inn i vårt nettverk? Det er fristende å sammenligne dette med hvem vi låser opp for og slipper inn gjennom inngangsdøra hjemme.

Informasjon om virksomheten og privatpersoner har også en verdi. E-postadresser blir videresolgt for å sende reklame, søkemotorer samler sammen våre søkeord for å se hva vi er opptatt av og kriminelle utnytter informasjonen til å begå ulovlige handlinger.

Nordmenn er mest på nett og tar raskt i bruk ny teknologi

I stadig økende grad kler vi på oss teknologien i form av klokker som viser aktivitet, berøringsarmbånd ment for avstandsforhold, BH-er som overvåker helsen, briller med nettfunksjonalitet, linser som overvåker blodsukker og parykker hvor man registrerer hjerneaktivitet. Tiden fremover vil vise hvordan vi vil greie å skape balanse mellom funksjonalitet, sikkerhet og «må ha»-faktoren til kroppsnær teknologi.

Informasjonssikkerhet er etter hvert blitt noe som «alle» må forholde seg til. Bloomberg har publisert statistisk materiale fra 2014 over utbredelsen av nettbruk og bredbånd i verden. Norge topper statistikken, hele 95 % av norske husholdninger er på nett.[1]

Privatpersoner og ansatte i virksomheter er mer og mer avhengig av IKT og internett-tilgang. Nordmenn generelt er raske til å ta i bruk ny teknologi, og mange bytter telefoner og PC-er fordi det har kommet en ny modell. Smart TV-er og vaskemaskin på nett er også blitt dagligkost i dag. Teknologi for trening, kosthold og helse er trendy, og mange er raske til å kaste seg på den nyeste teknologibølgen.

1: http://www.bloomberg.com/visual-data/best-and-worst/most-wired-in-the-world-countries

Tingene våre snakker

Tingenes internett eller Internet of Things (IoT) vil forenkle hverdagen vår. Tingene vi snakker om kommuniserer via internett, men er ikke bare en PC, nettbrett eller mobiltelefon. Dette er fysiske enheter som er koblet mot internett som for eksempel kjøleskap, låser, fjernstyring av varme, Smart TV, biler og vaskemaskiner.

Vi som bruker tingenes internett, legger igjen mye informasjon på internett. Summen av all informasjon som finnes på nett, kan si mye om en person og hvilke vaner vedkommende har. Store mengder data om forbrukere og deres atferd har en betydelig verdi for kommersielle aktører.

«Informasjon fra tingene våre kan derimot misbrukes til å begå kriminelle handlinger».

Industrien og forbrukerne må ta inn over seg hvilke konsekvenser internett tilkoblede produkter gir, slik at man kan ta hensiktsmessige forholdsregler.

Digitalisering av samfunnet

Internett åpner for et aktivt samspill mellom mennesker, tingene som omgir oss og informasjon. Vi vil se at dette i økende grad vil bli anvendt for å utnytte potensialet for verdiskapning og brukeropplevelse som ligger i teknologien. Neste generasjons velferdsteknologi vil i betydelig grad bygge på disse mulighetene. Likeledes digitaliseringen av det offentlige Norge. Fordelen vil være en døgnåpen forvaltning. Samtidig må vi erkjenne at massiv registrering og sammenstilling av informasjon, både vil sette personvernet under press og åpne for målrettet kriminalitet. Det vil også stille betydelige krav til tjenestetilbyderne om tilpasset funksjonalitet og sikkerhet i løsningene.

Digitaliseringen av samfunnet bidrar også til konkurransedyktig industri, man snak

Internet of Everything (IoE) benyttes som begrep for å beskrive et helhetlig digitalt samspill mellom mennesker, teknologi og informasjon. Den fysiske verden kombineres med den virtuelle verden. Dette bidrar til verdiskapning og effektivisering, både hos industri og forbrukeren, ved effektive produksjonsprosesser og tilpassede produkter.

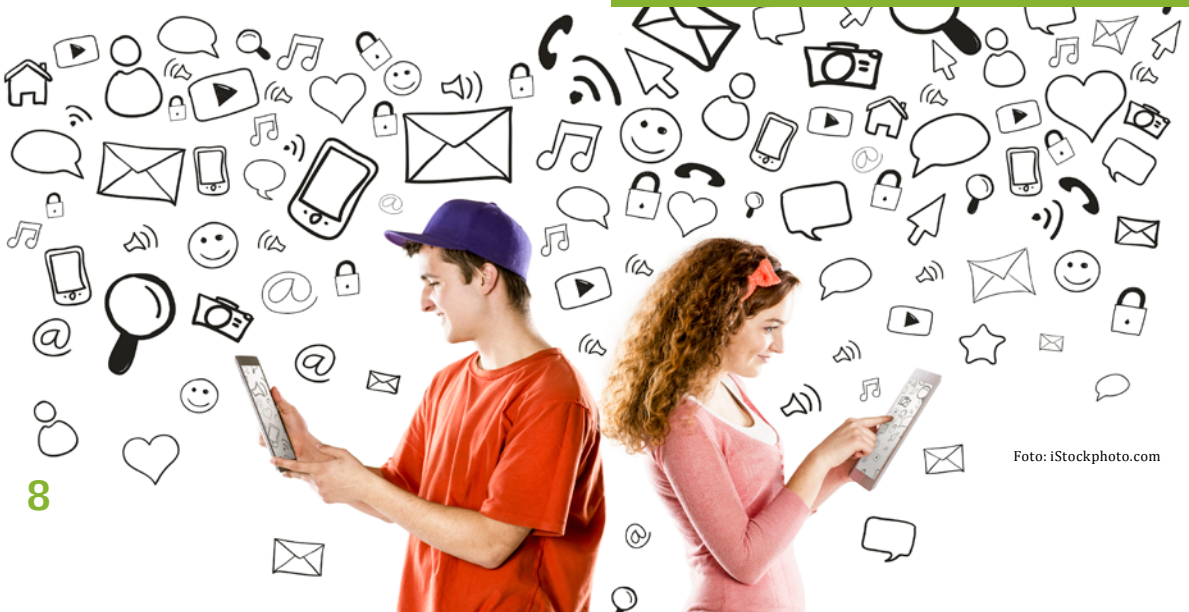


Foto: iStockphoto.com

Aktuelle eksempler

I analysen har NorSIS tatt utgangspunkt i teknologiske trender, reelle hendelser og samfunnsutviklingen for å gi en antakelse om utviklingen i nær fremtid. Tendenser og trender basert på våre analyser er illustrert ved eksempler.

«En kvinne har kjøpt seg ny, fin bil. Når hun våkner neste morgen er bilen borte fra garasjen. Det viser seg at en innbruddstyv har hacket kontrollsystemet til bilen ved hjelp av en app på mobilen. Damen finner igjen bilen ved hjelp av en sporingsapp på sin mobil. Hun anmelder forholdet til politiet og oppgir hvor bilen er parkert.»

Biler styres i dag av elektroniske kontrollenheter (ECU), og kommuniserer via kjøretøyets interne nettverk, kalt CAN bus (Controlled area network). Biler leveres ofte i dag med nøkkelløs adgang og start. Nøkkelen og bilen snakker sammen med radiosignaler. OBD, On Board Diagnostics, er en standard tilkoblingsmulighet og system for elektronikk i biler. Dette er bilens «hjerne» og her lagres feilkoder. Det er dette systemet et bilverksted benytter når man skal finne feilkoder.

Foto: iStockphoto.com

«En mann har brutt seg inn i postkasser i bygårder og stjålet en lang rekke bankkort samt brev med PIN-koder, bank ID-brikker, pass, skattekort, ordrebekreftelser, medlemskort og lønnsslipper.»

Med tilgang på alle disse dokumentene har mannen svindlet banker og butikker for store beløp i kontanter, varer og tjenester. Ofrene fikk livet snudd opp ned, og mannen kunne operere i over tre år før han ble stoppet. Mannen ble tiltalt for blant annet grovt bedrageri, krenkelse av identitet, grovt tyveri fra minibanker i inn- og utland, dokumentfalsk og heleri og er dømt til over tre års fengsel.

Identitetstyveri oppstår når noen anskaffer, overfører, besitter eller fremstår 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.

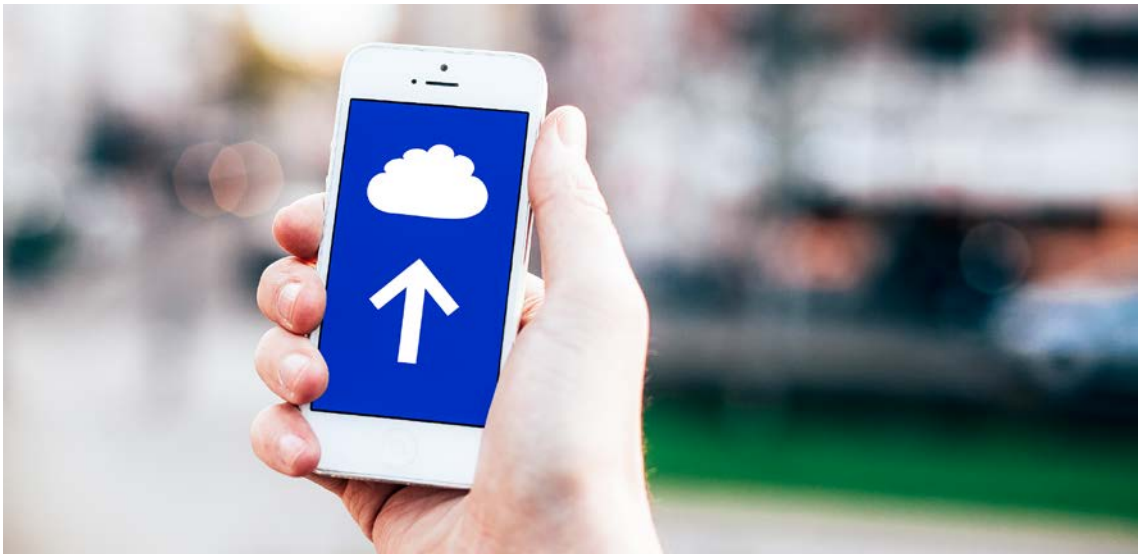
Foto: iStockphoto.com

««En mann har fått bankkort med NFC og kan betale uten PIN-kode. Kortet glemmes igjen i butikken og kortet benyttes på tre forskjellige bruker- steder og konto tappes for 600,–.»

NFC står for Near Field Communication, og er enkelt forklart en trådløs overføringsmetode. Metoden åpner for rask kommunikasjon mellom enheter med NFC-teknologi, og man kan lese av NFC-brikker. Baksiden av mobilen legges mot en annen mobil eller mot en betalingsteminal med NFC-brikke.

Foto: iStockphoto.com

«En leder benytter skytjenester for å dele dokumenter med sine medarbeidere. Virksomheten har sine anbud og prissetting av tjenester lagret i skytjenesten. En medarbeider sender ved en feiltakelse lenke til skytjenesten til en konkurrent. Konkurrenten har da full lesetilgang til alle dokumenter.»



«En underleverandør til et stort selskap har utviklet ny teknologi. Produktutvikler får tilsendt en e-post med vedlegg, angivelig fra Posten. Vedkommende blir nysgjerrig på hva dette er og klikker på vedlegget. Det hun ikke vet er at en konkurrent har sendt e-posten og at den inneholder et skjult spionprogram. Konkurrenten har nå tilgang til alle tekniske beskrivelser og tegninger av virksomhetens nyvinning.»

Foto: iStockphoto.com

«En ansatt har fått en e-post fra en samarbeidspartner. I e-posten er det et vedlegg som ser ut som en faks. Vedlegget er et løsepengevirus og alle filer på vedkommedes PC blir kryptert. Vedkommende har alle anbudsdokument lagret lokalt uten sikkerhetskopi. Anbudsdokumentene må rekonstrueres manuelt, noe som tar flere dager. Anbudsfristen går ut før arbeidet er ferdigstilt.»

Phishing, såkalt nettfisking, er angrepsmetode der kriminelle prøver å lure til seg opplysninger som kan brukes i vinningsøyemed. Eksempler er henvendelser på e-post der mottakeren bes oppsøke en webside eller klikke på et vedlegg. Formålet er å få mottaker til å gi fra seg personlig informasjon eller gi angriper tilgang til virksomhetens data.

Løsepengevirus låser alle eller noen filer på ofrenes PC med sterk kryptering. Ofrene får krav om å betale løsepenger for å låse opp innholdet.

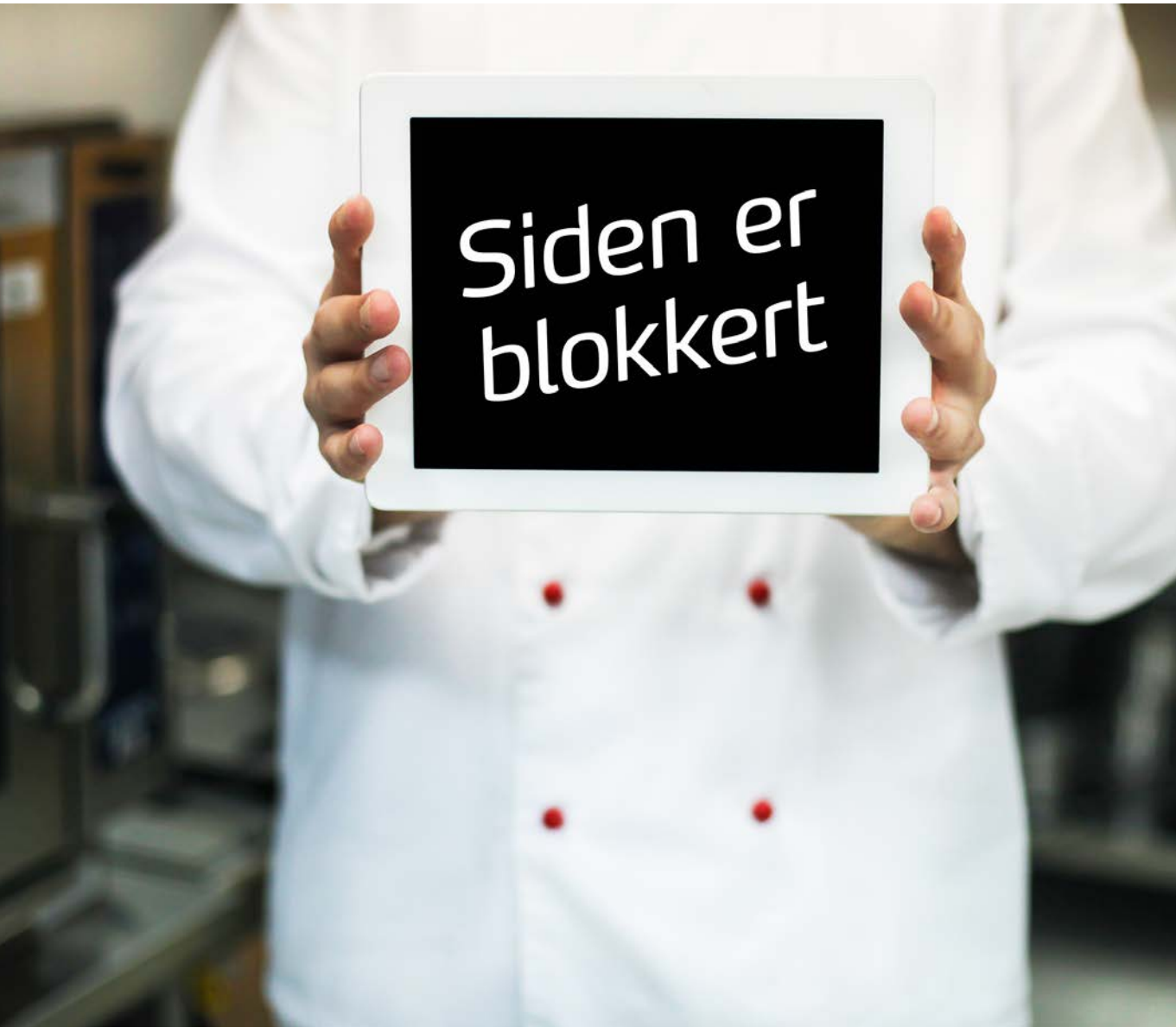
«For virksomheter og privatpersoner er det viktig å kjenne til teknologien, slik at du velger den teknologien som er mest sikker og hensiktsmessig for deg.».

«Norges utenrikspolitiske engasjement skaper reaksjoner i et ekstremistisk miljø. Hjemmesiden til en rekke små bedrifter blir gjort utilgjengelig samtidig. Flere andre virksomheter får hatske og ekstremistiske ytringer presentert på sine hjemmesider.»

Vandalisme mot websider, såkalt defacing, er angrep der noen bytter ut et element, tekst og/eller bilder på en webside for å påkalle brukerens oppmerksomhet. Man kan se på dette som en type graffiti på internett, men det kan også være politisk motivert.

DDoS, såkalt tjenestenektangrep, betyr at man sender massiv trafikk eller skadelige datapakker til en web-side. Web-siden takler ikke trafikken og bryter sammen. Hendelsen medfører at man ikke kan betjene kunder og man får ikke tilgang til data.

Foto: iStockphoto.com



Det farligste på nettet

er deg selv

Eksempler:

«En gutt tok et nakenbilde av kjæresten sin. Forholdet tok slutt og ekskjæresten delte bildet med en kamerat. Kameraten presset jenta for penger. Jenta brukte alle sparepengene sine på å betale, ellers ville nakenbildet bli publisert offentlig på nett…».

Foto: iStockphoto.com

Hevnporno: Mange unge, men også godt voksne mennesker deler nakenbilder og intime videoer med hverandre. Et nettfenomen er såkalt hevnporno, også kalt cyber-voldtekt. En forsmådd ekskjæreste, venn eller ektefelle deler bilder og videoer på internett for å hevne seg. Bildene spres gjerne jorda rundt, på egne pornonettsteder, blogger eller websider. 90 % av ofrene for hevnporno er kvinner, og 59 % av ofrene har fått publisert personlig informasjon sammen med bildene[2].

Utpressing: Ofre blir truet med at intime bilder vil bli publisert på nett hvis de ikke betaler penger for å slippe. En trend er utpressing fra tidligere kjærester og venner hvor man har fått bildematerialet av offeret selv. En annen trend er kriminelle som bryter seg inn i databaser og stjeler bilder, for så å presse offeret for penger.

«Creepshots» eller som vi på norsk kan kalle «snikbilder» er også en annen farsott på nett. Bilder med seksuelle undertoner, hvor den som er avbildet ikke har gitt samtykke, eller vet at man blir fotografert, spres på internett.

2: «Cyber Civil Rights»

Nettkriminalitet

– de usynlige truslene

Kriminaliteten fornyes i takt med at vi tar i bruk ny teknologi. Nettkriminalitet medfører betydelige utfordringer for samfunnet og ordensmakten. Mens kriminaliteten generelt er redusert, så ser vi at data-kriminaliteten øker. Økt bruk av internett kombinert med mangel både på sikkerhetstiltak og kunnskap om ny teknologi vil føre til økt kriminalitet via nettet[3]. Kriminaliteten utføres i det skjulte og skjer på tvers av landegrenser og uten fysisk tilstedeværelse. Gevinsten er høy og risikoen for å bli tatt er lav.

«Nettkriminalitet koster verdensøkonomien svimlende 3.000 milliarder kroner årlig».[4]

Hvem er de ulike trusselaktørene på nett?

Statsmakter

Cyberangrep utført av statsmakter kjennetegnes ved at det benyttes store ressurser på kartlegging, spionasje og sabotasje. Cybervåpen som Regin, utviklet som et spionasjeprogram og Stuxnet, utviklet for sabotasje, har forårsaket stor skade for de som ble rammet. Utvikling av avanserte cybervåpen krever betydelig kompetanse og store økonomiske ressurser. Flere nasjonalstater har iverksatt programmer for å utvikle slike våpen. Cybervåpen anvendes stadig mer målbevisst og effektivt i internasjonale konflikter.

Terrorister

Ekstremister og terrorister benyttet tradisjonelt internett til rekruttering og for å spre sitt budskap. Vi ser derimot en utvikling hvor enkelte grupperinger er i ferd med å bygge opp evne til cybersabotasje. Foreløpig virker viljen å være større en evnen. Forsøk på ødeleggelse er derfor rettet mot mindre virksomheter hvor sikkerhetstiltakene er lave.

Darknet

Et nett som benyttes til både legal og illegal informasjons-deling. Nettverket setter ikke fotspor i form av IP-adresser som vanlig internett, men er bygget opp av et intrikat system av datamaskiner. Darknet er ikke ulovlig å bruke og kan blant annet benyttes til fortrolig kommunikasjon. Anonymitetet i nettet gir imidlertid kriminelle tilgang til å spre barne-porno, omsette narkotika, identitetspapirer og våpen, med liten sannsynlighet for at myndingheter avslører aktørene.

3: Politiet: Anmeldt kriminalitet og straffesaksbehandling 2014

4: Center for Strategic and International Studies

Kriminelle
Datakriminalitet vokser raskt. Datakriminelle er ute etter penger eller informasjon som er omsettelig. Kredittkortinformasjon og personlig informasjon kan selges, på lik linje som fysiske produkter. De kriminelle kan utnytte stjålne identiteter for å kjøpe varer og tjenester på kreditt. Industrispionasje og informasjonstyveri skjer gjerne ved at ansatte blir lurt til å trykke på vedlegg og bilder i e-poster. Målrettede angrep rettes som regel mot ledere og ansatte med privilegerte rettigheter, da dette gir de kriminelle størst tilgang til virksomhetens informasjon.

Aktivister
Aktivister benytter nettet til å profilere og spre sitt gjerne politiske budskap. Angrepene skjer gjerne som nettbaserte protestaksjoner, og DDoS-angrep, såkalt tjenestenektangrep. Alt fra statsmakter til virksomheter man har et dårlig forhold til kan bli utsatt for såkalte «hacktivister». Det seneste eksempelet på slike handlinger er 19.000 franske websider som i uken etter terrorangrepet på satireavisen Charlie Hebdo ble utsatt for hackerangrep. Angrepene ble utført som tjenestenektangrep, og skjedde vilkårlig mot det som synes å være websider med sårbar programvare. Alt fra ideelle organisasjoner til kirker og småbedrifter ble angrepet. Det er umulig å forutsi hvem som er målet for aktivister, noe handlingene i etterkant av terrorangrepet på Charlie Hebdo viste.

Vandaler
Nettvandaler er ute etter å sabotere, gjøre hærverk, stenge nettsider, installere ondsinnet programvare for moro skyld, eller gjør digital ugang fordi man kan. Vandalismen kan være målrettet eller vilkårlig, og skjer i hovedsak mot organisasjoner og virksomheter.

Plageånder og mobbere
Plageånder på nett, også kalt troll, krenker andre ved ondsinnet og ufin atferd på nett. Det kan være kommentarer til innlegg, bilder eller blogger. Den krenkende atferden kan være målrettet mot enkeltpersoner, men kan også skje mot vilkårlige personer i et forum. Målrettede krenkelser karakteriseres som digital mobbing. Slik atferd skjer gjerne i det skjulte med anonyme avsendere, og gjerne flere sammen. Hevnaksjoner og ønske om å såre personer kan føre til at man legger ut intime bilder og personlig informasjon uten tillatelse.

Cyberangrep, industrispionasje og produktkopiering vokser raskt. Dette er globale utfordringer og omfatter alle virksomheter, små som store. Det er viktig å vite om trusselbildet og trusselaktørene for å kunne beskytte sin informasjon på best mulig måte.

Litt å tenke på

Det er ofte feilene brukeren gjør eller blir manipulert til å gjøre som utgjør de største farene og konsekvensen.

NorSIS arbeider for at alle skal kunne bruke internett og IKT trygt på jobb og privat. Vi er både samarbeidspartner og pådriver overfor myndigheter og virksomheter.

NorSIS er et uavhengig organ som ønsker å gjøre informasjonssikkerhet til en naturlig del av hverdagen, gjennom å:

- bevisstgjøre om trusler og sårbarheter
- gi råd om sikringstiltak gjennom nyheter, råd og veiledninger
- påvirke til gode holdninger innen informasjonssikkerhet

NorSIS målgruppe er innbyggerne og norske virksomheter i privat og offentlig sektor. Vi samarbeider med en rekke virksomheter i informasjonsarbeidet, skaper møteplasser og er tilrettelegger av nasjonal sikkerhets-måned. Alle samfunnsgrupper og media skal kunne dra nytte av våre tjenester.

En viktig del av NorSIS sin virksomhet er slettmeg.no, som er en gratis rådgivnings- og veiledningstjenesten for de som føler seg krenket på nett. En annen viktig tjeneste er IDtyveri.info, som gir verdifull informasjon om hvordan beskytte seg og hva man skal gjøre hvis man blir utsatt for ID-tyveri.

NorSIS
Norsk senter for informasjonssikring

Studievegen 2
2815 Gjøvik
Org.nr: 995 195 003

Telefon: 40 00 58 99
Nett: www.norsis.no
E-post: post@norsis.no

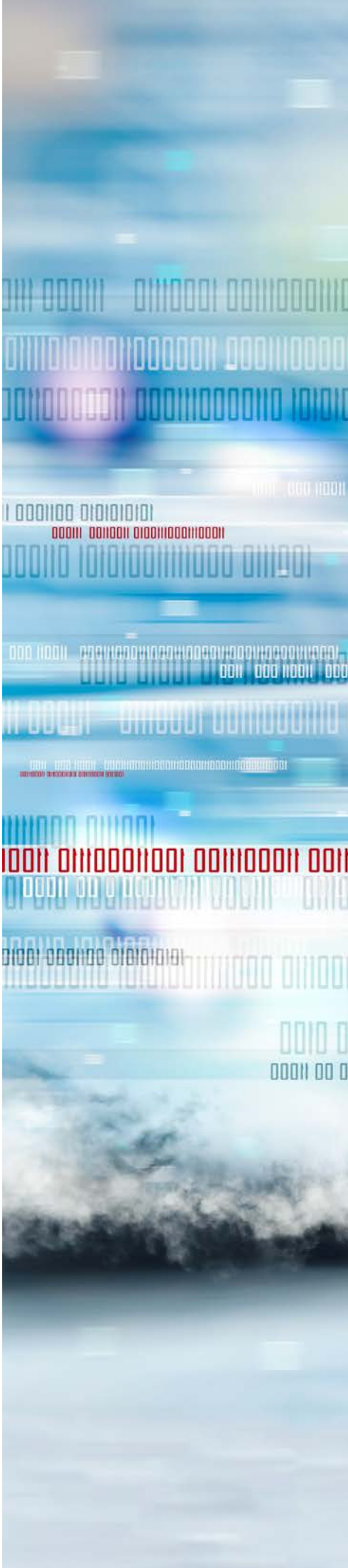


Foto: iStockphoto.com