2014

Mørketallsundersøkelsen

- Informasjonssikkerhet, personvern og datakriminalitet

NSR NÆRINGSLIVETS SIKKERHETSRÅD

Innhold

1 Innledning

Næringslivets Sikkerhetsråd (NSR) har som formål å forebygge kriminalitet i og mot næringslivet. Et av virkemidlene er å informere om de kriminelle og sikkerhetsmessige trusler og trender vi ser og forventer i fremtiden. Mørketallundersøkelsen™ har en sentral plass i opplysningsarbeidet mot næringslivet og offentlige myndigheter.

Mørketallsundersøkelsen™ 2014 er den 9. undersøkelsen som foretas av NSR gjennom Informasjonssikkerhetsutvalget (tidligere Datakrimutvalget). Undersøkelsen er enestående i Norge og er et viktig bidrag til å kartlegge omfanget av IT-sikkerhetshendelser, samt omfanget av sikringstiltak i norske virksomheter. Årets undersøkelse har i større grad enn tidligere fokusert på "hjelp til selvhjelp" til offentlige og private virksomheter gjennom anbefalinger og forslag til grunnleggende tiltak for hva virksomhetene kan gjøre for å beskytte seg bedre. Alle svar er anonymisert. Spørreundersøkelsen er gjennomført elektronisk av Opinion i perioden 3. mars til 10. april 2014. Tidsrommet for kartleggingen er kalenderåret 2013. Analysen er utført av Informasjonssikkerhetsutvalget, som i 2014 består av:

- Janne Hagen (Forsvarets forskningsinstitutt FFI, leder)
- Johnny Mathisen (Telenor)
- Vidar Østmo (Broadnet)
- Ole Tom Seierstad (Microsoft)
- Christophe Birkeland (Blue Coat Norway)
- Tønnes Ingebrigtsen (Mnemonic)
- Mari Grini (Alliansesamarbeidet SpareBank1)
- Tore Larsen Orderløkken (NorSIS)
- Eiliv Ofigsbø (Kripos)
- Hans Pretorius (Nasjonal Sikkerhetsmyndighet NSM)
- Martha Eike (Datatilsynet)
- Kristine Beitland og Arne Simonsen (NSR)

- Robin Stenvi (NorSIS, sekretær)

Utvalg og populasjon: Undersøkelsen ble utsendt til norske virksomheter i privat og offentlig sektor med 5 ansatte eller flere. Små virksomheter har 5-9 ansatte, mellomstore fra 10-99 ansatte og store virksomheter mer enn 100 ansatte. Utenfor undersøkelsen faller virksomheter som barnehager, barneparker, SFO, førskoler, kulturskoler, lønnet arbeid i private husholdninger, kinoer, borettslag, eierseksjonssameie, forening/lag/innretning, sokn/kirkelig fellesråd, og stiftelse m. fl. Det er trukket ut 6000 virksomheter til undersøkelsen. I bruttoutvalget er det 4500 private virksomheter og 1500 offentlige virksomheter. Totalt har 932 virksomheter svart på årets undersøkelse. Det gir en svarprosent på 15,5 % (mot 14,7 % i 2012 og 12,4 % i 2010).

Sammenlignet med 2012 er det en økning i andelen store virksomheter (fra 35 % til 46 %) og også en økning i andelen daglig ledere som svarer på undersøkelsen (oppgang fra 35 % i 2012 til 39 % i 2014). Endringene kan påvirke svarene.

2 Oppsummering av hovedfunn og anbefalinger

Slik stopper du en stor del av alle angrep*

- Oppgrader program og maskinvare
- Vær rask med å installere sikkerhetsoppdateringer
- Ikke tildel sluttbrukere administratorrettigheter
- Blokker kjøring av ikke-autoriserte programmer

*https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/systemteknisk-sikkerhet/s-01-fire-effektive-tiltak-mot-dataangrep.pdf

Store mørketall

Årets Mørketallsundersøkelse er basert både på anmeldte hendelser, innrapporterte hendelser i undersøkelsen og anonymiserte og aggregerte sensordata[1] om datainnbrudd fra NSM og Mnemonic[2]. Det er stor usikkerhet knyttet til mørketall både hva gjelder antall estimerte hendelser og kostnader som følge av hendelser. De få som rapporterer om økonomiske tap i undersøkelsen, melder om svært marginale tap. Analysen basert på hendelsene oppgitt i Mørketallsundersøkelsen™ viser store avvik mellom estimerte hendelser og anmeldte hendelser. Statistikk fra NSM viser at de i 2013 oppdaget eller ble varslet om 16000 hendelser, hvorav 5000 ble håndtert, av disse igjen var 51 alvorlige hendelser, i tillegg viser Mnemonics statistikker at deres kunder oppdaget 11000 hendelser. Loggdata fra disse to aktørene viser at en større andel virksomheter opplever datainnbrudd enn det som rapporteres i undersøkelsen. Det indikerer store mørketall mellom hva virksomhetene rapporterer av hendelser og hva de faktisk blir utsatt for. Sammenligning av sensordata og svar i gruppen store virksomheter viser at halvparten er utsatt for datainnbrudd i en eller annen form, og ikke bare 5 % slik det er rapportert av store virksomheter i undersøkelsen.

I år har undersøkelsen også satt søkelyset på personvern, men bare 5 virksomheter har rapportert personvernhendelser. Datatilsynet har selv 100 avviksmeldinger på hendelser som innebærer uautorisert utlevering av personopplysninger.

Undersøkelsen viser økt bruk av skybaserte tjenester; 2 av 3 virksomheter bruker nå skytjenester. Bruk av sosiale medier har økt fra 1 av 5 i 2010 til 2 av 5 i 2012 og 3 av 5 i år. Den viser også en utvisking av teknologigrenser mellom jobb og privatliv. Dette gjelder særlig bruk av privat mobiltelefon og nettbrett på jobb – her er det en fordobling siden sist. Undersøkelsen bekrefter mangelfull situasjonsforståelse og bestillerkompetanse på sikkerhet. 3 av 4 virksomheter har tillit til at data lagret i skyen er trygg, men 1 av 5 vet ikke hvor dataene blir lagret, og mer enn halvparten vet ikke om offentlige myndigheter har tilsynsrett. Dette er spesielt bekymringsverdig med tanke på personvern, da mange av systemene vil kunne inneholde personopplysninger.

Flere av svarene i undersøkelsen tyder på manglende kunnskap om informasjonssikkerhet. For eksempel svarer mange at de automatisk oppdaterer svitsjer og rutere til tross for at slikt utstyr typisk må oppdateres manuelt.

Truslene hardner til og sikringen må følge etter

Trusselvurderingene i denne rapporten vitner om et sammensatt trusselbilde der trusselen også kommer fra aktører med klart motiv, kompetanse og ressurser. Undersøkelsen viser at norske virksomheter ikke har oversikt over hvilke verdier de besitter. Selv i store virksomheter er det under halvparten som har gjort verdivurdering av informasjon. Tradisjonelle og modne sikkerhetstiltak er utbredt og IT-systemene er hos mange gjort mer motstandsdyktige teknisk sett sammenlignet med tidligere. De store virksomhetene er generelt bedre enn de små på dette området. Sett opp mot trusselbildet mener utvalget det er behov for å løfte kompetansen om informasjonssikkerhet, særlig i små virksomheter.

Utvalget gir følgende råd til norske virksomheter:

Forstå hvilken verdi informasjonen har for virksomheten din og hvordan informasjonen bidrar til verdiskapningen. Erkjenn at informasjonen også er attraktiv for andre utenfor virksomheten.

Ta i bruk et rammeverk for sikkerhetsstyring[3]. Sikkerhetsstyring handler om å ha en oversikt over verdiene virksomheten har og at man kjenner til risikoene og truslene virksomheten står ovenfor. Noen i virksomheten må ha ansvaret for dette.

Iverksett nødvendige tiltak. Tiltakene bør 1) være preventive, dvs. bidra til å unngå hendelser eller minske konsekvensen av hendelser; 2) bidra til oppdagelse av hendelser - uten overvåkning er man praktisk talt blind og vet ikke om man er utsatt for hendelser; og 3) være reaktive, dvs. bidra til å håndtere hendelser når de oppstår. Hvis man opplever hendelser, bør disse etterforskes og anmeldes.

1. Sensordata refererer til sensorer plassert ute i nettverket som samler inn informasjon om angrep.

2. Dataene er hentet fra to uavhengige kilder og det er uvisst hvor mye overlapp det er i dataene. Dataene kan derfor ikke summeres.

3. ISO 27001 og ISO 27002 er et rammeverk som er ofte brukt.

3 Risikobildet

Funnene i Mørketallsundersøkelsen™ gir ett bilde av informasjonssikkerhetstilstanden slik den er rapportert av virksomhetene. For å underbygge dette bildet har vi hentet inn trusselvurderinger fra eksperter på området.

Trusselvurdering fra Kripos

Bruk av teknologi gir kriminelle både markeder og nye verktøy for å begå kriminelle handlinger. IKT-kriminalitet omfatter kriminalitet som enten er rettet mot datasystemer og/eller datanettverk, eller der sentrale elementer av handlingsforløpet begås ved hjelp av datautstyr og/eller datanettverk. De to ulike kriminalitetsformene er ikke skarpt adskilt. De kombineres når hensikten med å begå et datainnbrudd er å skaffe tilgang til informasjon som senere kan brukes til å begå tradisjonell kriminalitet.

Det kan forventes en økning i IKT-kriminaliteten, samtidig som kriminelle naturlig følger den teknologiske utviklingen og benytter teknologi for å begå tradisjonell kriminalitet. Utviklingen skjer raskt, metodene blir mer avanserte og angrepene øker i omfang. Europol vurderer IKT-kriminalitet i form av angrep mot IKT-systemer, Internettbedragerier og seksuell utnyttelse av barn via Internettet som en økende trussel i Europa. I Norge er det også observert en slik økning. Dette innbefatter blant annet digital spionasje, hacking, salg av narkotika på nett, nettbankbedragerier og deling av seksuelle overgrepsbilder av barn.

Datainnbrudd utføres ved å utnytte sårbarheter og uautorisert å trenge seg inn i IT-systemer. [4]Hacktivister og kriminelle foretar dataangrep og skadeverk ved å sette datamaskiner ut av drift. Datainnbrudd, dataangrep og dataskadeverk skjer gjerne ved spredning av skadelig programvare (som virus og trojanere). Ondsinnet programvare spres i økende grad ved at den legges på Internettsider brukerne selv oppsøker. Når de besøker siden blir de infisert av den ondsinnede programvaren.

Både banker, interesseorganisasjoner og politiet melder at nettbankbedragerier er en vedvarende utfordring både i omfang og kompleksitet. Svindelforsøkene kommer gjerne i bølger. Selv om det har vært en nedgang av nettbanksvindel i Norge siste året, har man sett nye kampanjer i utlandet, og det er sannsynlig at norske banker vil rammes av nye svindelforsøk. De kriminelle er raske til å tilpasse sine metoder bankenes mottiltak.

Kortsvindel omfatter ofte svært høye beløp, er organisert og inkluderer mange typer modi – alt fra skimming, kopiering av kredittkort-informasjon og salg av stjålet kortinformasjon på Internettet. Organiserte kriminelle grupper bruker hackere og skadelig programvare for å stjele kredittkortinformasjon, og det finnes sofistikerte «svarte» markeder som bruker Internettet til å selge og handle med klonede bankkortdetaljer. Kriminelle følger pengestrømmen på nettet og i takt med at flere pengetransaksjoner digitaliseres og angriperne blir mer avanserte, er det sannsynlig at det vil komme omfattende, organiserte angrep som fører til store økonomiske tap.

Det har vært en eksplosiv økning av nye syntetiske narkotiske stoffer på det globale narkotikamarkedet. Disse nye stoffene markedsføres og selges gjerne via Internettet. Antall Internettbutikker som selger dette øker kraftig.

Det har vært en økning i antall tjenestenektangrep (også kalt DDoS – Distributed Denial of Service) i Norge. Tjenestenektangrep er et elektronisk angrep gjennomført over Internettet, som forhindrer at brukere får tilgang til nettsteder eller systemer. Langt flere enn målet blir derfor rammet i slike angrep.

Kriminelle oppholder seg i stadig større grad i skjul på Internettet, gjerne der de i tillegg får muligheten til å være anonyme (såkalt "Deep Web" og "Dark Nets"). Her kan man blant annet kjøpe narkotika, våpen, ulike former for dataangrep og finne flere fora for deling av seksuelle overgrepsbilder av barn. Dette brukes både av økonomisk motiverte kriminelle, som kortsvindel, og av personlig motiverte kriminelle, som for eksempel deler overgrepsbilder av barn eller kjøper ulovlige varer. Det er sannsynlig at organiserte, kriminelle grupper vil utnytte dette i større grad. Det er meget sannsynlig at det vil dukke opp andre alternativer som skal sikre anonymitet blant kriminelle i takt med at myndighetene klarer å stenge ned de kjente nettene.

Den enorme mengden bilder og personlig og sensitiv informasjon som ligger på nett skaper et poten-

4. Aktivister som bruker datateknologi for å spre sitt budskap, i dette tilfellet her, kriminelle handlinger med datamaskiner.

siale for trusler og utpressing mot enkeltpersoner, virksomheter og myndigheter. Vi kan vente at dette blir vanligere i fremtiden. Nettskytjenester og anonymiserte nettverk skaper også store utfordringer for politi- og kontrollmyndigheter, ettersom det er vanskelig å få tak i denne informasjonen, men det er på en annen side også viktig at ikke all informasjon er transparent. Dette er et dilemma i forhold til personvern og etterforskning av datakriminalitet.

De som utøver datakriminalitet utgjør ikke noen ensartet gruppe. Kriminaliteten som utføres omfatter alt fra relativt små lovbrudd til organisert kriminell aktivitet. Ondsinnet programvare er i dag lett tilgjengelig. Den utvikles og produseres av datakyndige, delvis til eget bruk, men selges også på Internett slik at ordinære databrukere lett får tilgang til og kan benytte programvaren til kriminell aktivitet. Ny teknologi gir politiet både utfordringer og muligheter. IKT-kriminalitet utføres uavhengig av landegrenser, internasjonalt samarbeid er derfor avgjørende for å lykkes.

Risikobilde fra NSM

NSM har gjennom flere år sett en tydelig og jevn økning av målrettede angrep mot norske interesser, både offentlig og privat. I 2013 ble det avdekket 51 alvorlige hendelser, noe som med stor sannsynlighet kun er en liten del av det totale antallet alvorlige hendelser i Norge. De 51 alvorlige hendelsene som NSM NorCERT håndterte i 2013 var en kombinasjon av hendelser avdekket gjennom NSM sitt eget sensornettverk VDI og hendelser hvor de berørte virksomhetene selv tok kontakt med NSM for bistand.

Man må kunne anta at mørketallene for slike angrep er såpass store at de teknisk sett kan være vanskelige å oppdage. En stor andel blir derfor ikke oppdaget av virksomheten som faktisk blir angrepet.

Den jevne økningen av målrettede angrep, som NSM har sett igjennom de siste årene, endret seg første halvår 2014. NSM ser nå en markant økning av angrep mot norske interesser. Dette er målrettede angrep hvor angriperen har et tydelig ønske om å hente ut informasjon fra virksomheten. Dette kan være dokumenter som beskriver høyteknologi eller forhandlings- og kontraktsdisposisjoner. Samtidig viser første halvår færre tjenestenektangrep (DDoS). Denne type angrep er fortsatt til stede i statistikken, men man har de siste årene sett en økt robusthet i norsk infrastruktur som har redusert antall vellykkede tjenestenektangrep.

Selv om økningen av målrettede angrep er bekreftet, kan man ikke se om antallet trusselaktører er økende, eller om de eksisterende aktørene har gjennomført flere angrep sammenlignet med tidligere.

Men noen fellestrekk kan vi se ut fra det totale antallet vellykkede angrep. Ett av hovedfunnene er hvordan vellykkede angrep benytter kjente sårbarheter for å få tilgang til data. Det er kun unntaksvis at «ikke kjente sårbarheter», 0-dags sårbarheter, blir utnyttet. Stort sett er det klienter eller servere som «burde» vært oppdatert som blir utnyttet.

I tillegg benytter målrettede angrep stort sett e-post som første vei inn for å skaffe fotfeste i organisasjonen. Dette er da ofte målrettet e-post (spearphising) som inneholder informasjon som oppfattes som relevant for brukeren. Denne informasjonen om e-post-mottakeren blir hentet ut gjennom analyser av informasjon på åpne kilder eller gjennom infiserte nettsteder som brukeren besøker regelmessig.

Et siste hovedfunn er at når trusselaktøren har etablert fotfeste gjennom utnyttelse av sårbarheter i kombinasjon med e-postmottakerens legitime rettigheter, er trusselaktøren meget vanskelig å oppdage. Det krever høy kompetanse for å oppdage at trusselaktøren har fått fotfeste, men det er også vanskelig å se at data forlater organisasjonen da dette skjer gjennom legitime trafikkprotokoller og i små mengder slik at trafikken er vanskelig å oppdage.

Trusselen fra Botnets – en vurdering fra Microsoft

En av de største truslene på Internett slik Microsoft ser den, er fra Botnets (Robot Networks). Botnetstrusselen spres via virus. Et Botnet er en samling datamaskiner som er infisert med programvare for fjernstyring, og et Botnet kan variere fra noen tusen til flere millioner infiserte maskiner. De kriminelle kan leie ut en eller tusen infiserte maskiner og fjernstyre disse til å begå kriminelle handlinger.

Virus spredningsmåter	Andel
Aktivert av brukerens handling	44,8 %
Automatisk kode (infisert fra USB-minnebrikke)	26,0 %
Automatisk kode (infisert fra nettverk)	17,2 %
Infisert fil	4,4 %
Gammel kjent sårbarhet hvor det finnes oppdatering	3,2 %
Nyere sårbarhet hvor det finnes oppdatering	2,4 %
Passord er knekket	1, %
Makroer	0,3 %
0-dag-sårbarhet uten oppdatering	0,1 %

Det er helt klart at det er økonomi som driver de kriminelle til å fortsette med sine aktiviteter, og en av de viktigste metodene som benyttes er å opprette og administrere Botnet. De handlingene som en kriminell kan gjøre med et Botnet er mange, fra annonsesvindel (din maskin registrerer mange klikk på en annonse, og annonsøren må betale deretter, selv om du ikke har klikket på annonsen), til tjenestenektangrep (DDoS) på web-tjenere. Angrep på alle typer organisasjoner har økt de siste årene, også i Norge.

Et Botnet er også et effektivt verktøy for ID-tyveri, de kriminelle kan overta hele din identitet, utgi seg for å være deg og til og med få utstedt nye kredittkort i ditt navn. ID-tyveri brukes også i målrettet angrep mot virksomheter, og det er da spesielt ledelsen som er målet. I hendelser omkring industrispionasje og økonomisk svindel brukes ID-tyveri i stor grad.

Når Botnet er et såpass stort problem på dagens Internett, må det gjøres nasjonale og internasjonale tiltak for å stoppe og ta ned Botnet, finne bakmenn og få renset maskinene som er infisert slik at de ikke lenger er ufrivillige deltagere i et kriminelt nettverk.

Et viktig tiltak for å unngå at maskiner blir en del av et Botnet, er å unngå å bli smittet av ondsinnet kode som rekrutterer din maskin til et kriminelt nettverk. Omtrent 45 % av infeksjonene skyldes at vi gjør en aktiv handling (klikker på koblinger i meldinger/e-post, åpner infiserte vedlegg i e-post eller at en web-side som besøkes er infisert). Bevisstgjøring og opplæring er det viktigste hjelpemiddel vi har for å unngå å bli en del av slike nettverk. En annen ting er å holde all programvare oppdatert til enhver tid, dette gjelder operativsystem, produktivitetsprogrammer så vel som tillegg som Java og Flash. Oppdatert antivirus og gode søppelpostfiltre på e-post er også viktige tiltak.

Malwaretrender 2014 fra Blue Coat

Starten på 2014 har vært preget av pågående økonomisk kriminalitet utført av grupperinger som er svært hardføre og profesjonelle, samt et stort antall målrettede angrep utført mot høyverdimål.

Den økonomiske kriminaliteten domineres av grupperinger som bruker den kjente banktrojaneren Zeus[5]. Zeus blir vanligvis distribuert til ofre gjennom enten spam eller via websider som er trojaniserte slik at brukere kan bli infisert automatisk. Zeus eksisterer ikke alene – den finnes i et økosystem av

5. I 2014 har Zeus-varianten som kalles P2P Zeus dominert; dette er varianten som kan kontrolleres gjennom bruk av peer-to-peer teknologi.

annen skadevare som den enten assisterer eller blir assistert av. For eksempel er det vanlig at Zeus blir lastet ned av en mindre trojaner som kalles Upatre; og Zeus selv er benyttet for å installere et antall annen skadevare, blant annet løsepenger-trojanere. En av disse er den beryktede Cryptolocker, som krypterer filer slik at de ikke lar seg gjenopprette uten å betale.

Grupperingene som står bak denne kriminaliteten er sannsynligvis profesjonelle som har operert over flere år, og det er vanskelig å sette de kriminelle nettene ut av drift, til tross for enkelte storsatsinger fra Microsoft og andre aktører.

Et relativt nytt fokusområde for den kriminelle undergrunnen er det som kalles point-of-sale malware – dvs. skadevare som er laget spesielt for å stjele informasjon fra datasystemer brukt i varehandelen. Flere større innbrudd har skjedd på denne fronten; for eksempel innbruddet i den USA-baserte butikkjeden Target, der opptil 40 millioner kredittkortdata kom på avveier.

Dette året har vi også sett stor aktivitet med hensyn til målrettede angrep, og dette blir utført av grupperinger med ulik nasjonal tilhørighet. Målene for disse angrepene er i noen tilfeller militære/sikkerhetspolitiske. Dette gjelder for eksempel angrep som har utgangspunkt i India og Kina, der man i høy grad bekymrer seg for indre trusler. I andre tilfeller er det åpenbare økonomiske motiver bak angrepene.

Flere av disse angrepene har blitt oppdaget i sammenheng med utnyttelse av nye sårbarheter i utbredt programvare. 2014 har vært preget av flere alvorlige 0-dagssårbarheter. Microsoft Word hadde en sårbarhet i hvordan de håndterte RTF-filer som kunne bli utløst ved å åpne filen i Word. Grupperingen som først brukte denne sårbarheten er ikke eksakt identifisert, men vi vet at i ettertid har aktører fra flere land tilpasset seg denne metoden; for eksempel vet vi at en av Kinas mest aktive angrepsgrupper, Comfoo/LuckyCat-komplekset, allerede har utført angrep med slike filer. Vanligste distribusjonsmetode er e-post.

Nettleseren Internet Explorer har hatt en serie sårbarheter siste år, som har blitt fikset etterhvert. Imidlertid er det ekstra alvorlig når en slik sårbarhet blir utnyttet i større skala før Microsoft har tettet igjen sikkerhetshullene. Dette skjedde i slutten av april, da angivelig kinesiske aktører klargjorde og gjennomførte en serie angrep mot mål i finans- og militærindustrien. Sårbarheten utnyttet en svakhet i de fleste versjoner av Internet Explorer; brukere som besøkte ondsinnede websider fikk lastet ned noe som så ut som et bilde, men som også inneholdt ondsinnet kode. Selv om Microsoft like før hadde avsluttet støtte for Windows XP, valgte til slutt Microsoft å publisere ekstraordinære oppdateringer for alle sine nyere operativsystemer – inkludert XP.

Adobe Flash var også utsatt for flere sårbarheter som ble utnyttet i diverse målrettede angrep.

En av årets store sikkerhetsbegivenheter var nyheten om at OpenSSL, et populært programvarebibliotek brukt i mange av verdens mest besøkte nettsteder, hadde en sårbarhet, populært kalt Heartbleed. Denne sårbarheten gjorde det mulig å tappe nettstedene for informasjon; typisk dreide dette seg om brukernavn og passord, men det ble også vist at det i noen tilfeller var mulig å stjele serverens private SSL-sertifikat.

Dette medførte en storstilt oppdateringsprosess - et kappløp med tiden for å tette sikkerhetshullet før angripere fikk sikret seg for mye data. Mange større nettsteder har anbefalt skifte av passord i ettertid.

Selv om slike sårbarheter benyttes i målrettede angrep i begrenset skala, tar det vanligvis ikke lang tid før kriminelle tilpasser seg sårbarhetene og benytter dem til mange ulike former for økonomisk kriminalitet.

Trusselvurdering fra Mnemonic

Mnemonics kunder representerer alle typer virksomheter – offentlige så vel som private. Totalt dekker Mnemonics sikkerhetsmonitoreringstjenester over 250 000 arbeidstakere, hvorav flesteparten av disse befinner seg i Norge.

I løpet av 2013 varslet Mnemonic sine kunder om ca. 11 000 sikkerhetshendelser. Rundt 1 av 4 har vært utsatt for målrettede angrep, datalekkasje og/eller tjenestenektangrep. 2 av 3 har vært utsatt for uautorisert bruk av IT-systemer eller datainnbrudd. Hele 9 av 10 har blitt kompromittert av skadelig kode benyttet av organiserte kriminelle.

Det er sannsynlig at statlig-sponsede eller statlige-organiserte aktører står bak det som er målrettede angrep. Denne typen trusselaktører har til hensikt å tilegne seg spesifikk informasjon eller produkter. Disse hendelsene oppdages ofte lang tid etter angrepet har begynt, noe som bidrar til at det potensielle skadeomfanget er stort.

Mnemonic har vært direkte involvert i granskningen av flere alvorlige sikkerhetshendelser, og vår samlede vurdering er at norske virksomheter – offentlige så vel som private – har en overdreven tro på egen datasikkerhet. Mange virksomheter mener de selv har tilstrekkelig kompetanse og midler til både å oppdage og håndtere sikkerhetshendelser. Vår erfaring tilsier det motsatte.

2014 – Hva ser vi i horisonten?

Javas svanesang og økte angrep mot nettlesere: Programvaren Java har over lengre tid vært den desidert mest populære angrepsvektoren. I løpet av de siste årene har 0-dagssårbarheter raskt blitt implementert i angrepsverktøy, men det tok brått slutt i februar 2013. Vi nærmer oss nå ett år uten nye, kritiske Java-sårbarheter. Mnemonics vurdering er at flere faktorer har bidratt til endringen. For det første holder nyere versjoner av programvaren et generelt høyere sikkerhetsnivå, og brukerne blir stadig oftere presentert med advarsler når programvaren blir forsøkt kjørt. For det andre har sikkerhetsforskere i større grad enn før bidratt til å rapportere sårbarheter til utviklerne. Til sist har oppmerksomheten rundt sårbarhetene nådd frem til sluttbrukerne, som selv tar aktive steg for å oppdatere til versjoner som ansees som trygge.

Samtidig som Java faller ut av søkelyset har angrep mot nettlesere økt. Microsoft Internet Explorer utgjør hovedandelen av nettlesere i norske virksomheter, og vi er vitne til et våpenkappløp der angriperne utnytter svakheter. Utviklerne av Mozilla Firefox og Google Chrome har beveget seg over til automatiske oppdateringsregimer med kortere utviklingsintervaller, mens Internet Explorer primært oppdateres på månedlig basis. I tilfeller hvor nye sårbarheter raskt blir tatt i bruk av angripere risikerer virksomheter i verste fall å være eksponert i flere uker. Automatisk oppdatering av nettlesere med korte utviklingsintervaller som for eksempel i Mozilla Firefox og Google Chrome, vil være et viktig virkemiddel for å beskytte mot angrepskode fremover.

Slutt for Windows XP: Microsoft Windows XP nådde «end-of-life» den 8. april 2014. Dette medfører at Microsoft ikke lenger vil publisere sikkerhetsoppdateringer til operativsystemet. Sårbarheter i populære systemer som ikke lengre blir oppdatert er svært verdifulle. Uavhengig om disse blir solgt til høystbydende, eller publisert direkte på nettet, forventer vi å se økt utnyttelse av Windows XP i tiden fremover.

Nye generiske toppnivådomener: I løpet av 2014 og 2015 forventer vi stor aktivitet rundt ICANNs nye generiske toppnivådomener (gTLD)[6]. Til tross for økt fleksibilitet for virksomheter som ønsker tilstedeværelse på nettet, åpner de samme mulighetene for skade på omdømme og svindel. Misfornøyde kunder, konkurrenter og aktivister kan enkelt registrere nærliggende domener (f.eks. firmanavn.group), eller domener som har til hensikt å skade omdømmet (f.eks. yourcompany.sucks). Det samme gjelder svindlere, som enkelt kan kjøpe domener som kan benyttes i svindelforsøk (f.eks. firmanavn.solutions/login).

Angrep mot det svakeste ledd i verdikjeden: Vi forventer å se økt angrepsaktivitet mot leverandører, partnere og andre tredjeparter som et ledd for å nå et spesifikt mål. En mindre underleverandør vil normalt sett ha mindre robuste sikkerhetsmekanismer og kontroller enn deres større kunder, og tilgang til nettverkene deres gir ofte gode infiltrasjonsmuligheter. Vi er kjent med bruk av denne taktikken mot norske virksomheter, noe som viser viktigheten av å vurdere sikkerheten hos samarbeidspartnere og leverandører.

6. http://newgtlds.icann.org/en/

4 På vei mot skyen? Bruk av IT og digitale tjenester

Spørsmålet om nettskytjenester ble introdusert i Mørketallsundersøkelsen™ 2012. Årets undersøkelse har fulgt utviklingen, og for første gang sett bruk av skytjenester opp mot behandling av personopplysninger.

CRM og kundeopplysninger

CRM-system (Customer Relationship Management System), kan på norsk kalles kundehåndteringssystem. Et CRM-system inneholder personopplysninger og omfattes av personopplysningsloven. Personopplysninger er alle opplysninger og vurderinger som kan knyttes til en enkeltperson. Ofte bruker virksomheter skytjenester for CRM-systemet, dette kan komme i konflikt med personopplysningsloven. Personopplysninger kan være opplysninger om ansatte, kunder, klienter eller pasienter. Virksomhetene som behandler personopplysninger, skal ha et formål med behandlingen. Et eksempel på formål kan være å ha oversikt over kundene til virksomheten, samt administrasjon av kjøp og salg.

En virksomhet som behandler personopplysninger gjør dette vanligvis etter samtykke fra den det samles informasjon om. I slike tilfeller kreves det utfyllende og konkretisert informasjon som setter den registrerte (kunden) i stand til å vurdere om vedkommende ønsker å gi sitt samtykke.

Det er normalt alltid virksomhetens leder som er ansvarlig for korrekt håndtering av personopplysninger. Personopplysningsloven stiller krav om at den som behandler personopplysninger skal etablere et system for internkontroll. Det betyr at virksomheter, som omfattes av loven, må iverksette systematiske tiltak for å sørge for at loven og tilhørende regelverk følges.

Les mer om personvern: http://www.datatilsynet.no/personvern/

Bruk av nettskytjenester

Bruken av nettskytjenester har gått betraktelig opp fra halvparten av virksomhetene i 2012 til at nå 2 av 3 virksomheter benytter seg av en eller annen form for nettskytjeneste. 1 av 3 virksomheter benytter seg av tjenester som er gratis (gmail, dropbox etc) i tillegg til betalingstjenester. Det er ingen store forskjeller mellom offentlig og privat sektor. En tredjedel av virksomhetene benytter seg ikke av noen form for nettskytjeneste.

I 2012 svarte halvparten av virksomhetene at de ikke hadde planer om å ta i bruk skytjenester innen de neste 12 månedene. Resultatene fra årets undersøkelse viser at 7 av 10 virksomheter ikke har planer om å ta i bruk skytjenester, noe som kan forklares med en sterk økning av bruk av skytjenester de siste to årene. Det er også store forskjeller basert på virksomhetens størrelse. Hos de minste virksomhetene sier 2 % at det er planer for å ta i bruk slike tjenester, mens blant de største er det 1 av 4 som har slike planer de neste 12 månedene. Det er også et skille mellom offentlige og private virksomheter når det gjelder planer fremover; 80 % offentlige virksomheter sier de ikke har slike planer, mens 67 % private virksomheter sier at det ikke finnes planer for bruk av nettskyen.

Av de som helt eller delvis setter ut IT-driften til andre (63 %) er det kun 1 av 6 som sier at de benytter slike tjenester i utlandet. Dette tallet er omtrent det samme som for to år siden. Det er, ikke overraskende, særlig de store virksomhetene som benytter seg av outsourcingtjenester i utlandet. Nesten 1 av 4 svarer bekreftende på dette. Det er også stor forskjell mellom private og offentlige virksomheter; 6 % av de offentlige virksomhetene som outsourcer IT-driften sier at de benytter slike tjenester i utlandet, mens for de private er tallet 20 %.

Endret bruksmønster

Dette skjedde: Et universitet hadde en elektronisk mappe med saksdokumenter i tilsettingssaker liggende åpent på Internett. Logger viste at opplysningene ble fanget opp av søkemotorer (Google, Bing, Yandex og Ephorus) og lastet ned i utlandet. Dokumentene inneholdt personalopplysninger, vurderinger og fødselsnummer om to personer og lå tilgjengelig på nett i tre måneder. Bakgrunnen for avviket var bruk av iPad med feil oppsett av en ansatt ved et av fakultetene. Den direkte årsaken til avviket er at rutine for oppsett av iPad via programmet Goodreader på en ansatts iPad ikke var korrekt fulgt. Programmet var satt opp med en toveiskommunikasjon mot server. Dette førte til at lokal mappe på iPad har blitt lastet opp på server med åpne leserettigheter.

Hvordan det ble oppdaget: En leder ved en av seksjonene i fakultetsadministrasjonen ved det aktuelle fakultetet ble gjort oppmerksom på at det lå en mappe med saksdokumenter i tilsettingssaker for ansatte åpent i deres system for nettpublisering.

Spesifikke tiltak som kunne hindret hendelsen: Virksomheter må gjøre en risikovurdering ved endringer i informasjonssystem som inneholder personopplysninger. I dette tilfellet skulle det ha vært gjort en vurdering av bruk av iPad og bruk av apper for dokumenter med personopplysninger. Virksomheten skulle videre ha kommet frem til tekniske og organisatoriske tiltak for å unngå at slikt skulle skje.

Tilgangsstyringen har ikke vært god nok. Oppsett av iPad skulle som standard vært satt opp med enveiskommunikasjon for kun nedlasting fra server. Dersom det skal åpnes for toveiskommunikasjon skal det være en aktiv handling fra en administrator på serveren. Automatisk oppsett av iPad med begrensede rettigheter kan gjøres som et teknisk tiltak. Rutiner og opplæring i bruk av iPad og Goodreader er organisatoriske tiltak for å unngå menneskelig svikt.

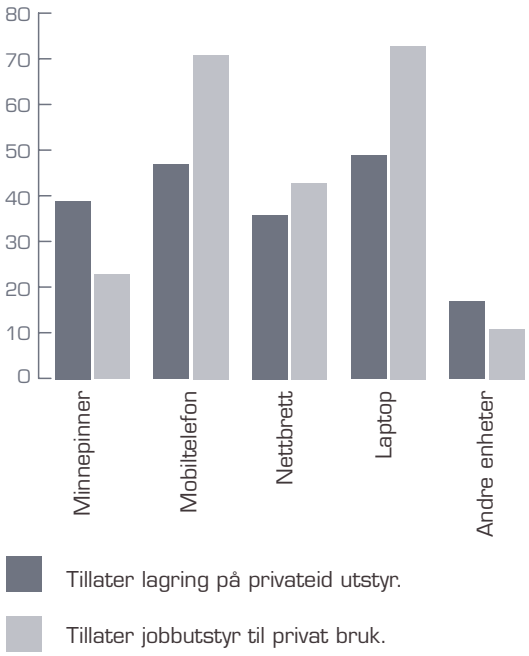
Det er en tydelig trend at samarbeidspartnere og leverandører i stadig større grad får tilgang til virksomhetens interne nett og IT-systemer utenfra. I 2010 svarte 1 av 3 at dette var tilfelle, mens i år svarer nesten halvparten bekreftende på dette spørsmålet. Det er særlig innen de små og mellomstore virksomhetene at det har skjedd en endring i løpet av disse årene, men det er fortsatt i de store virksomhetene at dette er mest utbredt. Der svarer 3 av 5 bekreftende, som i 2010. Trenden er den samme for offentlige og private virksomheter. For de private har andelen økt fra 38 % til 51 % på disse fire årene, mens offentlige virksomheter har økt fra 28 % til 39 %.

Som for to år siden svarer 3 av 5 virksomheter bekreftende på at de er avhengig av Internett som kommunikasjonsløsning mellom avdelingskontorer og/eller datterselskaper. Denne avhengigheten er naturligvis størst blant de store virksomhetene der 3 av 4 svarer bekreftende.

Det blir mer og mer vanlig å bruke privateid utstyr for lagring og behandling av virksomhetsinformasjon. Det er en kraftig økning i bruken av alle typer privateid utstyr, og for flere av utstyrstypene er det snakk om en fordobling i bruken i løpet av de to siste årene, eksempelvis mobiltelefon som har økt fra 23 % til 47 % og nettbrett som har økt fra 17 % til 36 %. Økningen gjelder alle typer virksomheter, enten de er store eller små, private eller offentlige, så det er tydelig at BYOD-trenden (Bring Your Own Device) også har nådd Norge.

Det er vanlig å behandle virksomhetsinformasjon på privat utstyr, men det er enda mer utbredt å benytte virksomhetens utstyr til private formål. Det gjelder særlig mobiltelefoner og laptoper, 7 av 10 tillater å bruke disse privat. For nettbrett, minnepinner og andre typer enheter er tallene noe lavere, men privat bruk av arbeidsgivers utstyr er mer utbredt desto større virksomheten er. Som eksempler kan nevnes at blant de små virksomhetene er

4



det 4 av 10 som sier at de ansatte bruker arbeidsgivers mobiltelefon privat, mens hele 9 av 10 sier det samme blant de store virksomhetene. For nettbrett er tallene henholdsvis 2 av 10 og 6 av 10.

Sosiale medier blir i stadig større grad brukt til ekstern kommunikasjon - fra 22 % i 2010 til 39 % i 2012 og 58 % i år. Som for fire år siden er det fortsatt mer utbredt blant offentlige virksomheter enn for private virksomheter. For de offentlige har andelen økt fra 25 % til 63 %, mens de private har gått opp fra 20 % til 56 %. Særlig innenfor offentlig administrasjon er denne måten å kommunisere på mye brukt. Innenfor den bransjen svarer hele 72 % bekreftende på dette spørsmålet.

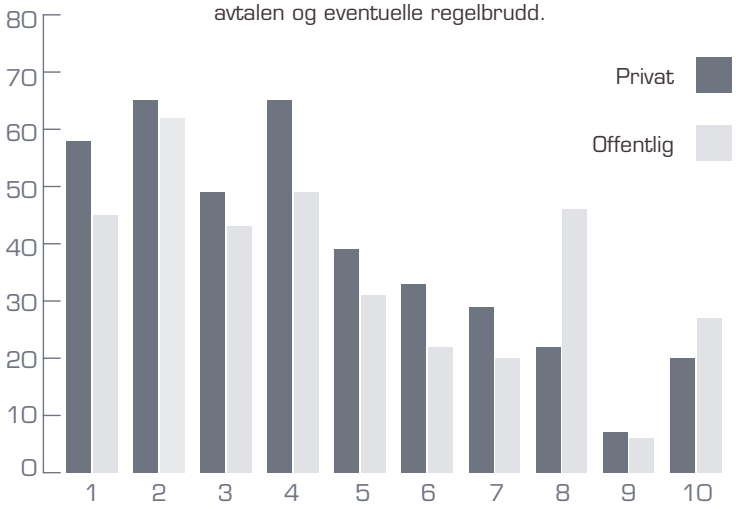
Avtaler med driftspartner/skyleverandør

Mye av informasjonen som lagres og behandles hos en driftspartner er underlagt regulativer og lover, det være seg personinformasjon, regnskapsdata, helsedata eller finansielle data. En avtale med skyleverandøren skal sikre at data behandles etter gjeldende regelverk.

Krav i avtalen

Elementer med i avtalen?	2010	2012	2014
Krav til tilgangskontroll til informasjon	57 %	54 %	54 %
Krav til taushetsplikt	68 %	67 %	64 %
Krav til tekniske sikringstiltak (kryptering etc.)	65 %	57 %	47 %
Krav til tilgjengelighet/oppetid	65 %	63 %	60 %
Rett til innsyn i relevante sikringsrutiner og dokumentasjon om f.eks. måling av sikkerhetsstatus	47 %	38 %	37 %
Kontraktsfestet et økonomisk ansvar ved informasjonssikkerhetshendelse eller manglende leveranser fra driftspartners side	31 %	26 %	30 %
Sanksjoner dersom krav ikke oppfylles	27 %	24 %	26 %
Databehandleravtale etter regler i personopplysningsloven §13 og Helseregisterloven §16	-	-	29 %
Vet ikke	14 %	25 %	22 %

Det er ingen store forskjeller i hva virksomheter kontraktfester av krav i år i forhold til tidligere år. De fleste områdene har en svak nedgang eller oppgang, med unntak av tekniske sikringstiltak, som har en nedgang på 10 % siden 2012. Dette kravet har falt jevnlig siden 2008. Et annet fremtredende trekk er at mens i overkant av halvparten av virksomhetene har krav om taushetsplikt i avtalen, er det bare 1 av 3 som har sanksjoner for å følge opp avtalen og eventuelle regelbrudd.



Årets undersøkelse avdekker at det er små forskjeller mellom små og store virksomheter når det gjelder kjennskap til innholdet i avtalen med driftspartner. Derimot er det større forskjeller mellom offentlige og private virksomheter: Private virksomheter har generelt større kjennskap til innholdet i avtalen enn offentlige virksomheter, med unntak av databehandleravtale.

Blant offentlige virksomheter har i underkant av halvparten krav til databehandleravtale, mens blant private er det kun 1 av 5 som har dette kravet. Det er også oppsiktsvekkende at 1 av 3 daglige ledere og 4 av 10 av økonomiansvarlige har svart «vet ikke» på disse spørsmålene. Hvis en virksomhet setter ut hele eller deler av behandlingen av personopplysninger til andre virksomheter, må forholdet etter personopplysningsloven reguleres i en databehandleravtale.

Hvordan kan leverandøren bruke dataene

1 av 5 vet ikke hvordan nettskyleverandøren kan bruke kundens data. Her skiller svarene seg basert på størrelsen på virksomhetene. De minste virksomhetene med under 10 ansatte har størst "vet ikke" respons (4

Elementer med i avtalen?	Privat	Offentlig
1. Krav til tilgangskontroll til informasjon	58 %	45 %
2. Krav til taushetsplikt	65 %	62 %
3. Krav til tekniske sikringstiltak (kryptering etc.)	49 %	43 %
4. Krav til tilgjengelighet/oppetid	65 %	49 %
5. Rett til innsyn i relevante sikringsrutiner og dokumentasjon om f.eks. måling av sikkerhetsstatus	39 %	31 %
6. Kontraktsfestet et økonomisk ansvar ved informasjonssikkerhetshendelse eller manglende leveranser fra driftspartners side	33 %	22 %
7. Sanksjoner dersom krav ikke oppfylles	29 %	20 %
8. Databehandleravtale etter regler i personopplysningsloven §13 og helseregisterloven §16	22 %	46 %
9. Nei, ingen av disse	7 %	6 %
10. Vet ikke	20 %	27 %

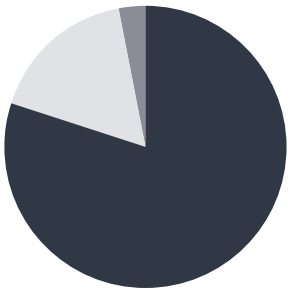
4

av 10), mens de største med over 100 ansatte har bedre oversikt og kjennskap til hvordan de ulike leverandørene behandler data (1 av 10 vet ikke). Når det gjelder bruk av kundedata svarer 3 av 4 at skyleverandøren ikke kan bruke disse dataene til andre formål.

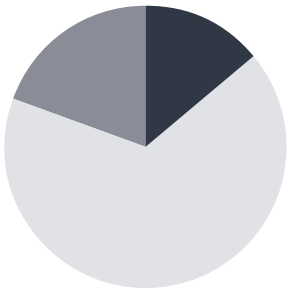
Tillit til skyleverandøren
Tillit til skyleverandørene og leverandørens evne til å beskytte data er høy; 3 av 4 av virksomhetene stoler på at leverandørene har rutiner for logging av uautorisert tilgang samt tilfredsstillende sletting av data om dette er aktuelt. Det er ingen store forskjeller mellom privat og offentlig sektor. De minste har en større andel av "vet ikke" svar (25 %) sammenlignet med de store (7 %). Tilliten til skyleverandører er høyest blant virksomheter som driver med forskning og utvikling (80 %).

Vet du hvor virksomhetens data fysisk blir lagret?
1 av 5 virksomheter vet ikke hvor virksomhetens data fysisk blir lagret. Av virksomheter med færre enn 10 ansatte er det 1 av 3 som ikke vet. Det kan tyde på at avtalene som blir inngått ikke godt nok beskriver hvor data fysisk blir lagret og under hvilken stats regelverk de behandles.

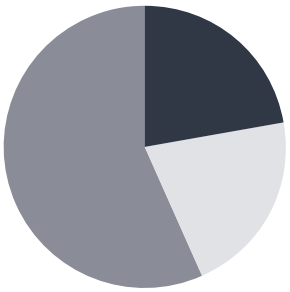
Det er ingen forskjeller innen bransje, geografisk tilhørighet og sektor.



Vet du hvor virksomhetens data fysisk blir lagret?



Blir virksomhetens data overført til andre land for redundans ved sikkerhetskopiering?



Regulerer avtalen tilsynsrett for offentlige myndigheter?

Overføring til andre land ved sikkerhetskopiering
1 av 5 virksomheter vet ikke om virksomhetens data blir overført til andre land ved sikkerhetskopiering. Større virksomheter er litt bedre enn små. Dersom det er personopplysninger, må virksomhetene vite om personopplysningene blir overført til andre land og hvordan personopplysningene blir behandlet der. De fleste virksomheter håndterer personopplysninger i større eller mindre grad (se tekstboks om CRM og kundeopplysninger). Personopplysninger kan ikke uten videre overføres til land utenfor EØS-sonen.

Regulerer avtalen tilsynsrett for offentlige myndigheter?
Over halvparten vet ikke om avtalen regulerer tilsynsrett for offentlige myndigheter, hos mindre virksomheter er andelen 2 av 3.

Av de som har svart Ja/Nei er det 7 av 10 av sikkerhetsansvarlige som vet om det blir regulert, mens blant de som innehar funksjon som daglig leder er det kun 4 av 10 som svarer Ja/Nei på samme spørsmål.

Datatilsynet gir ofte råd og veiledning om innholdet i databehandleravtaler, og slike avtaler er et viktig aspekt når en virksomhet skal vurdere om leverandører av skytjenester har god nok informasjonssikkerhet. Sammenlikner vi tallene med Datatilsynets erfaring med databehandleravtaler kan svarene tyde på at:

- avtalene ikke beskriver dette (godt nok)
- virksomhetene ikke kjenner innholdet i avtalen godt nok

Oppfølging av tjenesteleverandør

De små virksomhetene kommer svakest ut når det gjelder oppfølging av tjenesteleverandør; kun 1 av 5 svarer at de har avsatt ressurser til å følge opp eksterne leverandører. Kun 2 av 5 av virksomhetene i offentlig sektor har avsatt interne ressurser, i motsetning til halvparten i privat sektor.

Sett i lys av den underliggende trenden hvor man i stadig større grad benytter underleverandører til drift av IT-løsninger er det bekymringsverdig at tallene er så lave. Bestillerkompetanse er helt avgjørende for å sikre egne data hos en underleverandør. I en av fjorårets største sikkerhetshendelser, hvor en stor virksomhet ble helt "overtatt" av eksterne trusselaktører, var det virksomhetens underleverandør som ble benyttet som en vei inn til selskapet. Også tidligere år har kjeder av underleverandører vært benyttet for å nå frem til data hos en offentlig aktør.

Anbefalinger

Personopplysninger og skytjenester

Kartlegg og klassifiser alle systemer som inneholder personopplysninger innenfor virksomheten, fra sensitive til ikke-sensitive opplysninger. Gjennomfør risikovurdering av skytjenesten. Vurder databehandleravtalen mellom virksomheten (behandlingsansvarlig) og leverandøren (databehandler):

- Tilfredsstiller tjenesten kravene etter risikovurderingen?
- Ivaretar avtalen krav i henhold til norsk regelverk? Husk at din virksomhet fortsatt har ansvaret for at lovens krav følges.
- Sikkerhetsrevisjon
  - Påse at leverandør iverksetter tiltak og dekker hele kjeden
  - Dersom avtalen tilsier at en tredjepart skal utføre revisjon – krev å få se rapporten fra utført revisjon
- Vurder sikkerhetstiltak i avtalen
- Viktige problemstillinger:
  - Sikkerhetskopiering/Speiling - Hvordan fungerer dette?
  - Overføring til tredjeland: Personopplysninger kan ikke uten videre overføres til land utenfor EØS-sonen, men enkeltvise overføringer kan forhåndsgodkjennes av Datatilsynet. I tillegg er enkelte land godkjent av EU som trygge mottakerstater.
  - Sletting - Når slettes opplysninger hos leverandøren?
  - Tilgangsstyring – Er tilgangsstyring i samsvar med lovpålagte krav og egen internkontroll?
  - Dokumentasjon - Er løsningen tilstrekkelig dokumentert med hensyn til kontroll fra offentlige myndigheter?
  - Segmentering av databaser: Hvordan håndterer leverandøren at personopplysninger ikke skal sammenblandes mellom ulike behandlingsansvarlige?
  - Kan leverandøren bruke virksomhetens data til egne formål?
  - Leverandørens personvernvilkår (eller andre vilkår), må ikke gå utover databehandleravtalen.
  - Dataportabilitet - kan data overføres til ny tjenesteleverandør hvis det er ønskelig?
  - Sikker kommunikasjon – kryptering mellom:
    - Behandlingsansvarlig og databehandler (begge veier)
    - Datasentre
    - Databehandler og underleverandør (begge veier)

For mer informasjon: http://www.datatilsynet.no/Teknologi/Nettsky--Cloud-Computing/

Nettskytjenester har sine fordeler og ulemper når det kommer til sikkerhet. Tilgjengelighet blir lettere med nettskyen, samtidig som skalerbarhet, redundans og sikkerhetskopiering er mye mer naturlig. Infrastrukturen kan også bli sikrere; det konfigureres og oppdateres av noen som er eksperter på området. En av ulempene er at du mister noe av kontrollen; du vet ikke lenger nøyaktig hvor dataene lagres, og du må sørge for at kommunikasjonen og tilgangskontrollen er i orden.

- Dataene må klassifiseres. Du må med andre ord foreta en verdivurdering av dataene som skal behandles i skyen. Her må man være oppmerksom på hvilke lover man er underlagt. Har du ansatte er du underlagt personopplysningsloven.
- Ha en plan for identitetshåndtering.
- Utstyret som brukes for å koble til tjenesten må beskyttes (klientsikkerhet).
- Sørg for at du tilfredsstiller lover og regulatoriske krav.

"Veiledning for outsourcing av IT"[7] er en veiledning laget av NorSIS og NSR og er spesielt rettet mot små og mellomstore virksomheter.

7. Veiledning for outsourcing av IT: https://norsis.no/2012/07/veiledning-for-it-outsourcing/

5 Hendelser og mørketall

Estimerte mørketall

Mørketall er differansen mellom det reelle antallet hendelser norske virksomheter rapporterer å ha vært utsatt for i 2013, og det antallet hendelser som er anmeldt til politiet i samme periode. Mørketallsundersøkelsen™ omhandler også informasjonssikkerhetshendelser som ikke nødvendigvis kan regnes som straffbar IKT-kriminalitet. Estimatet av det totale antallet hendelser norske virksomheter har vært utsatt for er basert på opplysninger fra årets undersøkelse, samt SSBs statistikk over næringsstrukturen i Norge.

Ofre for kriminaliteten

Mørketallsundersøkelsen™ har gjennom flere år påpekt at de vanlige uttrekkene av statistikk fra politiets strafferegister (STRASAK) ikke skiller på om offeret for kriminalitet er virksomheter eller privatpersoner. Forholdene anmeldt av virksomhetene vil derfor reelt sett være enda lavere enn antallet anmeldelser som brukes i undersøkelsen. Utvalgets gjennomgang viser at, av 174 datainnbrudd anmeldt i 2013, er virksomheter ofre i 40 av dem. Statistisk sentralbyrå har i skrivende stund ikke publisert statistikk over *ofre for kriminalitet* i 2013, men sier følgende om dette for statistikken fra 2012:

> Det ble anmeldt nesten 394 000 lovbrudd i 2012. Foretak eller andre juridiske enheter ble registrert som fornærmet for 59 700 lovbrudd, og antallet lovbrudd med foretaksofre var i 2012 vesentlig lavere enn de tre foregående årene. Sammenlignet med året før er antallet lovbrudd med foretak som offer færre innenfor de fleste lovbruddsgrupper, og i antall er nedgangen størst for skadeverk. I 2012 var foretak registrert som offer for 38 200 vinningslovbrudd og 7 100 skadeverk.

Statistisk sentralbyrås statistikker over de forskjellige kategorier lovbrudd viser at foretak utgjør en høyere andel blant ofre for økonomisk kriminalitet og skadeverk enn de har i den samlede statistikken. Mørketallsundersøkelser supplerer derfor offentlig statistikk på området datakriminalitet.

Hendelsestype	Hendelser (estimat)	Anmeldelser
Datainnbrudd (hacking)	4000	174 (40)[8]
Misbruk av IT-ressurser	7300	61
Spredning av ulovlig/opphavsrettslig beskyttet materiale (piratkopiering)	2900	6
Totalt	**14200**	**241**

Tabellen viser estimater av antallet hendelser norske virksomheter var utsatt for i 2013, samt antallet anmeldelser av tilsvarende saker. Utvalget av hendelsestyper i årets undersøkelse er noe annerledes enn tidligere år, med et mer begrenset utvalg. Likevel bekrefter undersøkelsen nok en gang tidligere funn – at mørketallene er store. Dersom man justerer for det faktum at en stor del av de anmeldte sakene er saker der offer er privatpersoner, kan vi konkludere med at kun 1 % av den rapporterte datakriminaliteten mot norske virksomheter blir anmeldt til politiet.

8. 174 anmeldelser totalt, og 40 anmeldelser fra virksomheter.

Type hendelser

Det samlede bildet fra Mørketallsundersøkelsen™ viser at 4 % av norske virksomheter har vært utsatt for datainnbrudd i 2013, og at dette tallet holder seg relativt stabilt over tid. Videre viser undersø-

kelsen totalt sett at det samlede antallet hendelser har en nedgang.

Datainnbrudd er kanskje den mest konkrete og direkte formen for IKT-kriminalitet, og den som flest intuitivt vil kategorisere som IKT-kriminalitet. I følge Mørketallsundersøkelsen™ har det vært en liten økning av datainnbrudd sammenliknet med 2012, men fortsatt lavere enn i 2010. Antallet datainnbrudd for norske virksomheter er i undersøkelsen estimert til 4000 totalt, og kriminalstatistikken viser at 174 tilfeller er anmeldt til politiet i samme periode.

Misbruk av IT-ressurser har også hatt en svak økning fra 2012. Antallet hendelser med misbruk av IT-ressurser er estimert til 7300, mens kriminalstatistikken viser 61 anmeldte forhold i samme periode. Antallet anmeldelser har økt jevnlig siden 2011 og 2012.

Har virksomheten vært utsatt for noen av følgende informasjonssikkerhetshendelser i kalenderåret 2013?	**2010**	**2012**	**2014**
Datainnbrudd (hacking)	5 %	3 %	4 %
Dataskadeverk og bedrageri	-	-	3 %
Misbruk av IT-ressurser (PC/nett/server)	11 %	5 %	6 %
Spredning av ulovlig/opphavsrettslig beskyttet materiale (piratkopiering)	5 %	4 %	2 %
Tyveri av IT-utstyr (PC, server, nettbrett, smarttelefoner etc.)	18 %	13 %	17 %
Tap av opplysninger underlagt personopplysningsloven (personopplysninger på avveie)	1 %	1 %	1 %
Hendelse som har medført varsling fra Internet Service Provider (ISP)	-	-	5 %
Svindlet med bruk av falsk identitet (identitetstyveri)	-	-	2 %
Sosial manipulering	-	-	3 %

Rapporterte hendelser med spredning av ulovlig/opphavsrettslig beskyttet materiale (piratkopiering), viser en klar nedgang (halvering) fra 2012. Antallet tilfeller av piratkopiering i norske virksomheter estimeres til 2900, og kriminalstatistikken viser at kun 6 slike tilfeller ble anmeldt i 2013.

Tyveri av IT-utstyr er den kategorien hendelser norske virksomheter identifiserer som hendelsestypen de er mest utsatt for. Dette er også den enkleste typen informasjonssikkerhetshendelser å oppdage, siden hendelsen oppdages fysisk og ikke er avhengig av eksempelvis analyse av tekniske logger. Tendensen er økende fra 2012 (13 % til 17 %), nesten tilbake til 2010 nivå (18 %). Den generelle trenden er imidlertid at vinningskriminaliteten går ned, med andre ord en motsatt trend enn det virksomhetene rapporterer om i samme periode.

Men hvor pålitelige er disse dataene? Utvalget har gjort en sammenligning av oppdaget datainnbrudd for store virksomheter med flere enn 100 ansatte gjennom Mørketallsundersøkelsen™ og det Mnemonic og NSM oppdager gjennom sine sensornettverk og overvåkningssystemer[9] .

9. Her har vi kun sett på virksomheter over 100 ansatte, da dette utvalget er mer sammenlignbart med utvalget fra NSM og Mnemonic.

5

Datainnbrudd i store virksomheter	Mørketallsunder-søkelsen™	Mnemonic	NSM
Antall datainnbrudd	600	444	51
Andel virksomheter utsatt for datainnbrudd	5 %	66 %	50 %

Denne sammenligningen indikerer at norske virksomheter er utsatt for hacking i mye større grad enn det som rapporteres i Mørketallsundersøkelsen™. Automatiserte overvåkningssystemer og profesjonelt sikkerhetspersonell oppdager flere hendelser enn virksomhetene selv rapporterer. Mens 5 % av store virksomheter i Mørketallsundersøkelsen™ oppdager datainnbrudd, så oppdager Mnemonic datainnbrudd hos 66 % (2 av 3) av sine kunder. NSM oppdager datainnbrudd hos 50 % (1 av 2) av de virksomhetene som er tilknyttet deres overvåkingssystem.

Dette skjedde: En Liten virksomhet kontaktet NorSIS og fortalte at de hadde fått løsepengevirus (ransomware) på en av sine PC-er, denne ble brukt av administrasjonen og hadde viktig informasjon de måtte få tilbake. De hadde ikke sikkerhetskopi av maskinens interne harddisk så svært mye informasjon ble tapt. Dette eksemplet er ikke enestående, svært mange har blitt rammet av løsepengevirus der maskinen eller deler av harddisken har blitt kryptert slik at brukeren ikke har fått tilgang til filene. Bakmennene har så krevd penger for å gi brukeren passordet til de krypterte filene. I mange tilfeller har brukerne også blitt skremt ved at de har fått opp bilder på skjermen av politiets logo med beskjed om at de må betale en bot for ulovlig programvare for å få låst opp igjen systemet sitt.

Tiltak:

- Opplæring av brukere om åpning av vedlegg, lenker, surfing.
- Rutiner for sikkerhetskopiering og instruks for hva som ikke skal lagres på utstyr som ikke er med i sikkerhetskopieringen. Test at sikkerhetskopiering og gjenoppretting virker.
- Ikke betal – anmeld forholdet.

Veiledning fra NorSIS om 10 enkle tiltak for sikker PC-bruk. https://norsis.no/2012/06/sikre-pc-en-din/

Årsaker til ikke å anmelde

Årsakene til at virksomhetene ikke anmelder de hendelsene de rapporterer å være utsatt for er mange og sammensatte. Uten å kunne si at det peker seg ut et entydig eller klart bilde av årsaken til ikke å anmelde, fremstår følgende argumenter som de vanligste årsakene til at virksomhetene ikke anmelder: «Tror ikke det er mulig å finne gjerningsmannen», «Saken er ubetydelig», og «Saken er håndtert internt i virksomheten». Videre oppgir mange følgende årsak til ikke å anmelde: «Angrepet var ikke spesielt rettet mot vår virksomhet». En annen årsak til ikke å anmelde er i tillegg «Manglende tiltro til politiets kompetanse». Dette kan tyde på at politiarbeidet blir oppfattet å være organisert og innrettet i for stor grad mot tradisjonell kriminalitet og har ikke har klart å holde tritt med utviklingen.

Personopplysninger og mørketall

I Mørketallsundersøkelsen™ har vi kun fått innrapportert 11 hendelser fra 5 virksomheter relatert til personopplysninger på avveier. Vi har derfor altfor svake data til å estimere totale tall. Tall fra Datatilsynet på antall avviksmeldinger er imidlertid ca. 100 i året og tendensen er økende. Datatilsynet vet at overvekten av hendelser er rapportert fra finans og forsikring, og at en stor andel kan forklares ved feilaktige utsendelser (e-post og brev). Årsaken til at finans- og forsikring melder om flere hendelser enn andre bransjer kan være at bransjen har kultur for hendelsesrapportering iht. pålegg i IKT-forskriften, og ikke nødvendigvis at det oppstår flere personvernbrudd i denne bransjen enn i andre bransjer i Norge.

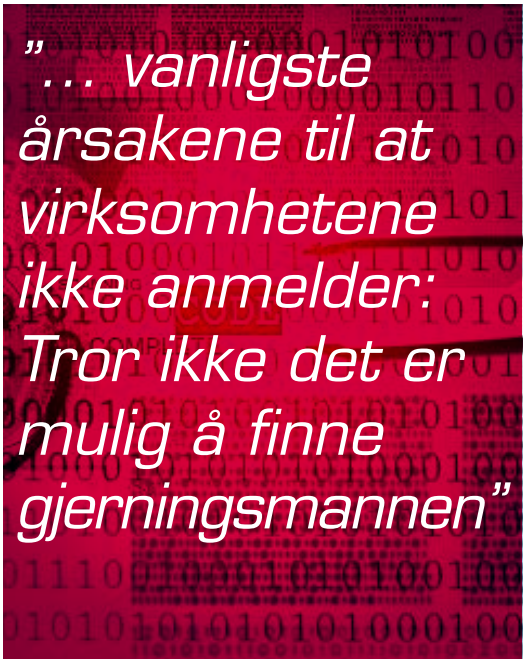
Hindre tilsvarende hendelser i etterkant

Blant de som har opplevd hendelser, både kriminelle handlinger og feilaktige handlinger (totalt 462 virksomheter), har 4 av 10 satt i gang "opplæringstiltak eller holdningsskapende" arbeid og / eller "forbedring av sikringsrutiner". Veldig mange angrep er helt eller delvis basert på menneskelig svikt i kombinasjon med mangel på teknisk sikkerhet, noe som trusselvurderingen fra Microsoft viser. Oppgang i opplæring og holdningsskapende arbeid er derfor positivt.

Hva er gjort for å hindre tilsvarende informasjonssikkerhetshendelser?	2010	2012	2014
Investering i tekniske sikringstiltak	31 %	33 %	38 %
Forbedring av sikringsrutiner	54 %	41 %	52 %
Flere personer og/eller mer tid til sikringsarbeid	5 %	10 %	12 %
Opplæringstiltak eller holdningsskapende arbeid	-	41 %	52 %
En total gjennomgang av sikringsnivå	16 %	12 %	14 %
Søkt råd hos private sikkerhetsleverandører/konsulenter	-	-	24 %
Søkt råd/kontaktet aktuell myndighet (eks. Datatilsynet, NSM, Finanstilsynet, Helsetilsynet m-fl)	-	-	10 %
Ingenting	16 %	12 %	11 %

Sammenlignet med tidligere år, så er resultatene positive. Flere av dem som har vært utsatt for kriminelle hendelser iverksetter tiltak. 1 av 10 gjør ingenting, denne andelen har gått stabilt ned siden 2010.

De som har vært utsatt for utilsiktede hendelser (tap av minnepinne, e-post sendt til feil adressat o.l.) er derimot ikke like flinke til å iverksette tiltak, 1 av 5 gjør ingenting. Kun 1 av 10 setter av flere personer eller mer tid til sikringsarbeidet. Dette har gått noe opp siden tidligere år, men er fortsatt lavt. IT- og sikkerhetsansvarlig svarer i mye høyere grad enn ledere at de iverksetter tiltak.



5

Informasjon på avveier

Som ved tidligere undersøkelser, er det e-post sendt til feil adressat som skjer oftest. Nesten en tredjedel av virksomhetene har opplevd e-post på avveier.

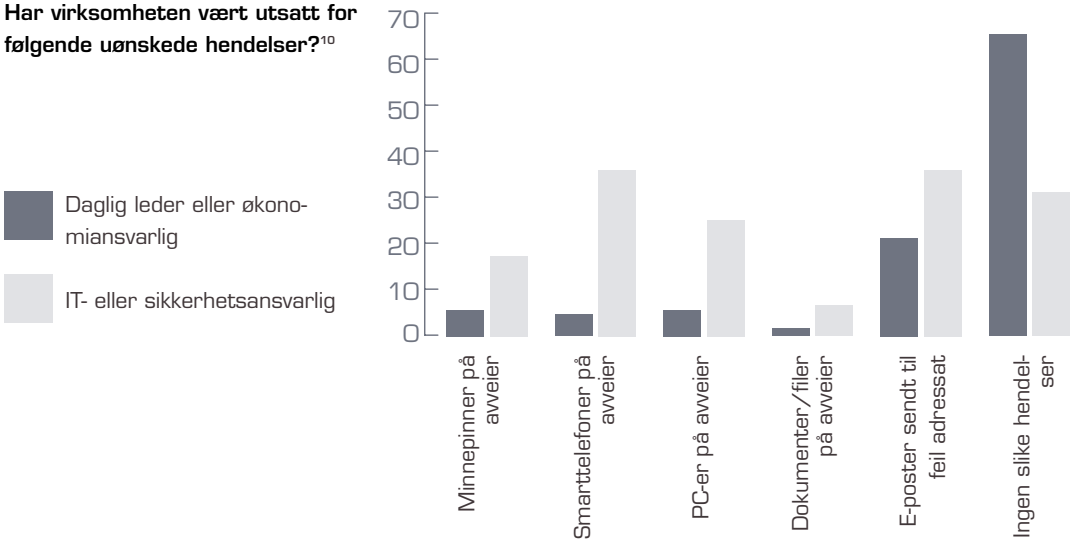
Sammenliknet med 2012 er det en økning i smarttelefoner på avveier (12 % til 20 %), mens minnepinner på avveier er redusert (26 % til 11 %). Forklaringen til dette er nok at flere lagrer dataene i skyen, og smarttelefoner blir mer og mer brukt mens bruk av minnepinner reduseres.

Halvparten av virksomhetene har ikke opplevd noen hendelser der IT-enheter eller informasjon kommer på avveier.

Har virksomheten vært utsatt for følgende uønskede hendelser?[2]	2012	2014
Minnepinner på avveier	26 %	11 %
Smarttelefoner på avveier	12 %	20 %
PC-er på avveier	12 %	15 %
Dokumenter/filer på avveier	16 %	4 %
E-poster sendt til feil adressat	32 %	29 %
Ingen slike hendelser	51 %	50 %

Hvis man ser på de største virksomhetene, så er det lite trolig at en tredjedel ikke har opplevd IT-utstyr eller informasjon på avveier. Dette kan tyde på manglende forståelse eller manglende oversikt. Dette kommer tydeligere fram når vi ser på hva forskjellige ansatte sier. Daglige ledere og økonomiansvarlige svarer i mye mindre grad at de opplever hendelser, i motsetning til IT-ansvarlig og sikkerhetsledere. 2 av 3 daglig ledere eller økonomiansvarlig sier de ikke har hatt noen hendelser, mens blant IT- og sikkerhetsansvarlige, så er det bare 1 av 3 som sier de ikke har hatt noen hendelser. Dette kan tyde på at ansatte som jobber med denne type hendelser har et mye bedre bilde enn daglig leder og økonomiansvarlig.

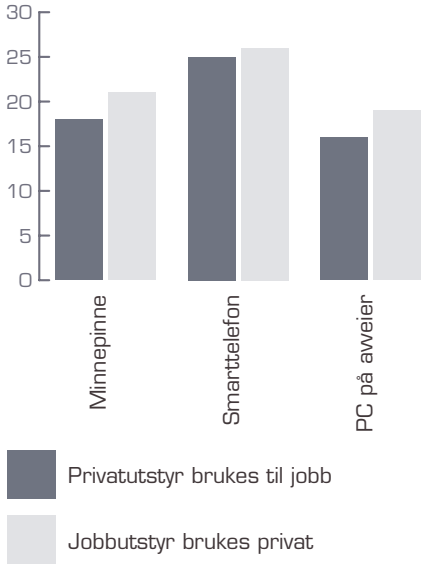
Har virksomheten vært utsatt for følgende uønskede hendelser?[10]



10. Spørsmål i 2012: Kan informasjon ha kommet på avveie i kalenderåret 2011 på grunn av?

Selv virksomheter som tillater at privat utstyr brukes på jobb eller at jobbutstyr brukes privat, har relativt få hendelser. Kun 1 av 6 som tillater at private PC-er brukes på jobben har opplevd at PC-er kommer på avveier. Det samme gjelder de som tillater at arbeids-PC brukes privat. Dette er riktignok høyere enn de som ikke tillater slik bruk, men fortsatt lavt. Dette kan tyde på at de ikke har kontroll over utstyret eller mangler rapporteringsrutiner, slik at man ikke vet at utstyr kommer på avveier.

Utstyr på avveier



Anbefaling

- Gjør grundige verdi- og risikovurderinger
- Etabler retningslinjer for hvordan tap av utstyr skal rapporteres. Dersom virksomheten tillater å lagre jobbinformasjon på privat utstyr så må man også lage retningslinjer for hvordan det skal håndteres.
- Mobile enheter, som smarttelefoner og nettbrett kan inneholde mye sensitiv informasjon. I tillegg er de lette å miste. Virksomheten må etablere tiltak for å beskytte denne informasjonen. Det anbefales å etablere opplegg for å kunne fjernslette informasjon når enheter kommer på avveier.

Konsekvenser og kostnader som følge av hendelsene

Svarene i Mørketallsundersøkelsen™ viser at blant de 462 virksomheter som har svart på dette spørsmålet, har bortimot 3 av 10 oppgitt ingen direkte kostnader og hele 4 av 10 oppgitt ingen indirekte kostnader som følge av kriminaliteten. Blant de 2 av 10 virksomhetene som har rapportert direkte kostnader har de fleste rapportert at de har mindre enn 10 000 NOK i tap som følge av datakriminalitet. Resten vet ikke om de har hatt tap eller har ikke estimert tapene. Av dette kan vi lese at norsk næringsliv ikke ser de økonomiske konsekvensene av datakriminaliteten. Som følge av stor usikkerhet knyttet til rapporterte tall kan vi ikke estimere pålitelige totale tapstall for Norge.

Utvalget har derfor sett på andre analyser av økonomiske tap som følge av datakriminalitet. Finanstilsynets risikoanalyse gir en oversikt over tapene knyttet til Internetthandel i Norge. Tapene representerer alle bankene i Norge og er innhentet av Finans Norge og Bankenes standardiseringskontor (BSK) i samarbeid med Finanstilsynet. I 2013 var tapene knyttet til misbruk av kort i forbindelse med Internetthandel beregnet til 51 mill NOK. Totale tap knyttet til betalingskort var 140 mill. NOK. I følge BSK gir dette likevel ikke det hele bildet: I tapsberegningen bør man også ta med investeringer og drift i forebyggende sikkerhet, men dette finnes det ikke tall på. Center for Strategic Studies (CSIS) har i samarbeid med sikkerhetsselskapet McAfee estimert kostnaden av datakriminalitet for en rekke land[11]. De norske tapene er anslått til 0,64 % av BNP, dvs. 19 mrd. for den norske økonomien.

Anbefaling til virksomheter

- Etabler rutiner for hendelsesrapportering[12] internt i virksomheten.
- "Veiledning i hendelseshåndtering" er rettet mot små og mellomstore virksomheter.
- Anmeld straffbare hendelser.

Anbefaling til myndighetene

- Politiets straffesaksregister (STRASAK) må utbedres i tråd med teknologiutviklingen.
- Politiets ressurser knyttet til IKT-kriminalitet må styrkes.
- Det operative og forebyggende samarbeidet mellom privat og offentlig sektor må styrkes.

11. Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II, Center for Strategic Studies, June 2014.

12. Veiledning i hendelseshåndtering: https://norsis.no/2012/07/hendlesesshandtering/

6 Anbefalte sikringstiltak

Risikostyring og sikkerhetsledelse

Hele 3 av 4 virksomheter gjennomfører risikovurdering ved anskaffelser eller betydelige endringer. Blant de største gjør 90 % denne analysen. Dette er omtrent som tidligere. Så høye tall på risikovurdering burde påvirket antall alvorlige hendelser positivt, men dette har ikke skjedd. En mulig årsak, som har kommet frem i flere av siste års alvorlige hendelser, er at den økte kompleksiteten i infrastrukturene og bruk av multisourcing-modeller har gjort at man mangler nødvendig oversikt over logisk og fysisk infrastruktur. Dette i sin tur medfører at mange av risikovurderingene blir gjennomført på svakt grunnlag. Hendelser, både villede og ikke-villede, har ofte utgangpunkt i en feil eller en sårbarhet hos en konkret fysisk komponent. Når man ikke har den nødvendige koplingen mellom egne verdikjeder, som ofte danner grunnlaget for risikovurderingen, og fysisk infrastruktur, vil man ikke få den ønskede gevinsten av egne risikovurderinger.

Enkel risikoanalyse for små virksomheter

Risikoanalyse trenger ikke å være en massiv prosess; man kan gjøre enkle risikoanalyser ved å tenke gjennom hva som kan skje med virksomheten og de verdier virksomheten har. Ta utgangspunkt i verdivurderingen av informasjon:

Trusler: Hva kan virksomhetens informasjonsverdier bli utsatt for? Dette deles ofte inn i tre kategorier: brudd på **konfidensialitet** – sensitiv informasjon holdes hemmelig, brudd på **integritet** – dataene er korrekte og pålitelige og brudd i **tilgjengelighet** – dataene er tilgjengelig når man trenger dem. Beskyttelse mot disse truslene vil ofte være motsigende, å sikre tilgjengelighet for eksempel vil ofte gi dårligere konfidensialitet. Her må virksomheten vurdere hva som er viktig.

Akseptabel risiko: Man greier aldri å sikre seg 100 %, derfor utsetter man seg alltid for en viss risiko. Virksomheten må vurdere hva som er akseptabel risiko og hva som er uakseptabel risiko.

Konsekvenser: Hvis en hendelse oppstår, hvilke konsekvenser får dette for virksomheten? Virksomheten bør stille seg selv slike spørsmål. Hvis en angriper får tilgang til vår kundedatabase (konfidensialitet), hvilke konsekvenser får det for oss, våre kunder og våre samarbeidspartnere? Hva er konsekvensen hvis jeg mister all informasjonen på min bærbare PC (tilgjengelighet)? Hva er konsekvensen hvis regnskapet inneholder feil informasjon (integritet)?

Risikovurdering: Total risiko synliggjøres ved å se på konsekvens og sårbarhet samlet. En grundig risikovurdering vil prøve å beskrive dette nøyaktig, slik at man vet hvor det er best å igangsette tiltak.

Tiltak: Hvis risikoen er større enn akseptabel risiko må man igangsette tiltak for å redusere konsekvensen eller sårbarheten. Både virksomheten og trusselbildet er i konstant forandring, så dette er en prosess som må gjøres jevnlig.

Organisatoriske tiltak

Det har vært en positiv økning i organisatoriske tiltak. 1 av 3 virksomheter sier at de identifiserer og klassifiserer virksomhetsinformasjon (verdivurdering). Det er en signifikant oppgang fra 1 av 6 i 2012. Andelen er likevel lav. Selv i store virksomheter er det under halvparten som sier de har gjort verdivurdering av virksomhetsinformasjon. Det samme gjelder krav til at det skal utpekes informasjonssikkerhetsansvarlig. Den organisatoriske modenheten i informasjonssikkerhet er lav.

Virksomheten har retningslinjer for:	2010	2012	2014
identifisering og klassifisering av virksomhetsinformasjon (verdivurdering)	20 %	16 %	35 %
sikker bruk av sosiale medier[13]	30 %	24 %	41 %
sikker bruk av mobiltelefoner, smarttelefoner, nettbrett, mediaavspillere, etc[14]	39 %	29 %	51 %
ansattes bruk av cloud/nettskytjenester for virksomhetsinformasjon	-	9 %	28 %

Nye brukstrender krever andre retningslinjer: Retningslinjer for sikker bruk av sosiale medier har økt fra 24 % til 41 %, retningslinjer for sikker bruk av mobiltelefoner, nettbrett etc. har økt fra 29 % til 51 % og retningslinjer for ansattes bruk av nettskytjenester, som Gmail og Dropbox har økt fra 9 % til 28 %. Dette er teknologier som også var utbredt i 2012, men sikringen henger litt etter. Store virksomheter er flinkere enn små.

Undersøkelsen viser også at virksomhetene har en vei igjen å gå når det gjelder styringssystem for informasjonssikkerhet og ikke minst opplæring av egne ansatte. Bare 2 av 10 gir sine ansatte opplæring gjennom ansettelsesperioden, og 4 av 10 ved nyansettelse.

Virksomheten har et rammeverk/styringssystem for informasjonssikkerhet som inneholder:	2010	2012	2014
retningslinjer for sikker drift av IT- infrastruktur (Backup, patching, herding, endringskontroll, mm.)	77 %	65 %	68 %
planer for håndtering av de viktigste informasjonssikkerhetshendelser	40 %	36 %	42 %
krav til gjennomføring av systematiske øvelser knyttet til IT-beredskap	11 %	15 %	20 %
oversikt over alle personopplysninger som behandles i virksomheten	56 %	53 %	56 %
oversikt og kontroll på brukeridentiteter med tilgang til virksomhetens system (tilgangsstyring)		-	69 %
rutiner for håndtering av personopplysninger (internkontroll)[15]	67 %	65 %	67 %
retningslinjer for håndtering av avvik (personopplysningsloven)		-	51 %
sikkerhetsinstruks for brukere, leder og sikkerhetsansvarlig		-	42 %
krav til at det utpekes en informasjonssikkerhetsansvarlig	57 %	26 %	26 %

Virksomheten har krav om at ansatte:	2010	2012	2014
skal gis opplæring i sikker bruk av IT ved ansettelse	42 %	42 %	40 %
skal gis opplæring i sikker bruk av IT regelmessig gjennom ansettelsesperioden	31 %	24 %	24 %
må undertegne retningslinjer for bruk av IT-systemer	34 %	35 %	42 %

13. Svar i 2010: nettsamfunn (Facebook, Second life etc.)

14. Svar i 2010: mobiltelefoner/smartphones

15. Spørsmål i 2010 og 2012: Etablert formelle rutiner for håndtering av personopplysninger?

Det er ca. 30 % som oppgir at de ikke har etablert noen rutiner for å følge opp etablerte retningslinjer. Dette tallet er ganske stabilt igjennom ulike sektorer og mellom offentlig og private virksomheter.

Anbefalinger

En god måte å arbeide med informasjonssikkerhet er å følge ISO 27001/ ISO 27002. Disse standardene gir retningslinjer som sikrer systematikk, dokumentasjon og rollefordeling. I bunn ligger risikovurderinger som fører til tiltak og / eller risikoaksept. Man behøver naturligvis ikke å ha til hensikt å sertifisere virksomheten for å følge standardenes metodikk.

Tekniske tiltak

Herding av IT-systemene har gått opp fra 2012 (56 % til 69 %). Kun 1 av 10 svarer nei på spørsmålet, en halvering fra 2012. Tre kategorier av tiltak har hatt en overraskende stor nedgang siden 2010, personlig brannmur på mobile PC-er (fra 64 % til 56 % til 51 %), kryptert kommunikasjon over usikre linjer (fra 61 % til 56 % til 43 %) og separerte sikkerhetssoner i nettet (fra 63 % til 61 % til 47 %). Noe av svingningen kan forklares av respondentens tolkning eller kompetanse; brannmur er nå blitt standard på de fleste PC-er og det er tvilsomt at kun halvparten har dette. En annen mulig forklaring er at brannmurer ikke har samme betydningen for sikkerheten som tidligere da mye ondsinnet programvare benytter protokoller som uansett er åpne i brannmuren, som eksempelvis http og https. Endring i spørsmålsstillingen over disse årene kan også ha medvirket til trenden.

Kun 1 av 5 krypterer bærbare media, tyveri av IT-utstyr er den mest utbredte formen for registrert IT-kriminalitet, så dette kan være et veldig nyttig tiltak.

Kunnskapen om tekniske sikringstiltak er relativt lav, i snitt er det 1 av 5 som svarer at de ikke vet om sikringstiltaket er tatt i bruk. Dette har hatt en jevn økning fra 2010. Dette er ikke spesielt overraskende, da det er en høyere andel av daglige ledere som svarer i årets undersøkelse.

Hvilke sikringstiltak brukes for å sikre virksomhetens informasjon og systemer/nettverk?	2010	2012	2014
Sentralisert konfigurasjonsstyring	-	67 %	60 %
Pålogging og adgang via fysiske autentiseringsmekanismer (f.eks. smartkort, token, etc)	26 %	39 %	28 %
Tekniske tiltak for behandling av sensitive data (f.eks. kryptering av e-post)	-	26 %	27 %
Nødløsning for kommunikasjon (alternativer for data- og telekommunikasjon)	-	33 %	39 %
Flere versjoner av sikkerhetskopier av data	-	-	70 %
IT-systemene herdes (settes opp etter beste kjente sikkerhetspraksis)	54 %	56 %	69 %
Administrasjonsrettigheter på PC er fjernet	41 %	45 %	43 %
Personlig brannmur på mobile pc-er	64 %	56 %	51 %
Kryptert kommunikasjon over usikre eksterne linjer[16]	61 %	56 %	43 %
Separerte sikkerhetssoner i nettet[17]	63 %	61 %	47 %

16. Svar i 2010 og 2012: Virtuelt privat nettverk (VPN)

17. Svar i 2010 og 2012: Ulike sikkerhetssoner i nettet

Fortsettelse fra s 24: **Hvilke sikringstiltak brukes for å sikre virksomhetens informasjon og systemer/nettverk?**	2010	2012	2014
Filter mot uønsket web-trafikk	70 %	69 %	62 %
Kryptering av bærbare media	23 %	24 %	20 %
Avlåst datarom	72 %	70 %	67 %
Duplisering av kritiske komponenter	53 %	49 %	54 %
Innbruddsdetekteringssystem (IDS)	30 %	26 %	33 %
Reservestrøm, UPS	71 %	66 %	69 %

Oppdatering

Det er ikke forskjeller i oppdateringsrutinene for virksomheter basert på bransje og geografisk tilhørighet. Det er, som i tidligere undersøkelser, større forskjeller mellom størrelse på virksomhetene.

Så å si alle har i dag tatt i bruk antivirus. Også når det gjelder oppdatering av antivirus viser resultatene at jevnlig oppdatering av denne ligger stabilt, og det har ikke variert signifikant de siste fire årene. For alle spurte svarer 9 av 10 at de enten oppdaterer automatisk, når oppdateringer foreligger eller regelmessig. Sluttbrukeren er mest direkte eksponert for trusselen fra ondsinnet programvare, og det er derfor lettest å forholde seg til denne. Men også her viser små virksomheter et dårligere tall, 86 % opp mot 96 % i store virksomheter. Det er bekymringsverdig siden de små gjerne har minst evne, økonomi og støttesystemer til gjenoppretting dersom skade skulle skje.

Oppdatering av operativsystemer viser liten utvikling. 3 av 4 svarer at operativsystemer oppdateres automatisk, periodisk eller når det foreligger oppdateringer. Også her viser små virksomheter svakere tall og ligger på 59 % sammen med virksomheter innen helse og sosial og overnattings- og serveringsvirksomhet, som er helt nede på 54 %.

Oppdateringen av annen programvare viser samme trend. 1 av 10 av virksomheter under 10 ansatte og 4 av 10 virksomheter med over 100 ansatte oppdaterer programvare regelmessig. Det lave tallet kan skyldes at man i de mindre virksomhetene ikke forstår eller har personale til å vedlikeholde programvareoppdateringer.

Rutere og svitsjer må oppgraderes manuelt. Undersøkelsen viser tydelig at større virksomheter er langt flinkere til å følge med på dette utstyret og oppgradere når det er nødvendig. Forståelsen her er at oppetid og tilgjengelighet er viktigst om det ikke finnes kjente sårbarheter i dette utstyret. Dette krever selvfølgelig at man følger med i trusselsituasjonen og følger anbefalinger fra sine leverandører.

Anbefaling

Operativsystemer og flere programmer støtter nå automatisk oppdatering. Bruk automatisk oppdatering der produktet har støtte for det. For annet utstyr som ulike applikasjoner og nettverksutstyr bør man forstå funksjonen og bruken av disse og være kjent med trusselsituasjonen ved enten å sørge for å ha avtale med operatøren, eller forsikre seg om at driftspartner følger opp viktige oppdateringer.

Vær særlig på vakt ved installasjon av gratisprogrammer da man altfor ofte for noe «på kjøpet». Be IT eller sikkerhetsavdelingen sjekke ut all programvare som skal installeres på virksomhetens utstyr.

Sikkerhetslogger

Logging er et viktig hjelpemiddel både for å avdekke kriminell aktivitet, finne kilde til innbrudd og finne feil og sårbarheter i dine systemer. Uten logger, verktøy og kunnskap til å kunne analysere disse kan

man fort stå på bar bakke og være blind. Tallene taler for seg selv, og de viser en urovekkende trend for virksomheter under 100 ansatte. Ved forrige undersøkelse i 2012 sa 8 % av virksomheter under 100 ansatte at de ikke logget. I år har denne andelen økt betydelig, til gjennomsnittlig 15 %. Store virksomheter derimot, har blitt langt bedre. I 2012 var det 6 % som ikke logget - i år er tallet nede på 2 %. Store og mellomstore virksomheter gjennomgår loggene regelmessig. Økt sikkerhetsfokus kan ha fått store virksomheter til å rette blikket mot loggene. For store virksomheter over 100 ansatte har faktisk dette tallet økt med 10 prosentpoeng.

Tallene for offentlig og privat virksomhet viser at prosentandelen "Vet ikke" har økt for private virksomheter, mens den har sunket for offentlige, som kom svært dårlig ut i undersøkelsen fra 2012. Private virksomheter logger også langt mer regelmessig enn i forrige undersøkelse, mens offentlige ligger på samme nivå. Man kan undres om fokuset på sikkerhet og viktigheten ved å ha oppmerksomhet på mekanismer som kan avsløre sikkerhetshendelser er forbedret i offentlige virksomheter, mens implementeringen av systemene ikke er kommet ordentlig i gang.

Anbefaling

Når man først har et sikkerhetsbrudd kan dette ofte kun spores og etterforskes på bakgrunn av logger fra sikkerhetsutstyr, brannmurer, webproxyer, antivirus, server og tilsvarende. Om logger fra disse ikke er tilgjengelige er det i mange tilfeller umulig å vurdere hva årsaken til innbruddet er, og det er slett ikke lett å vurdere hvilke tiltak man skal gjøre for å sikre videre drift. Ofte pågår et innbrudd over uker, måneder og kanskje til og med år før det blir oppdaget. Da er det viktig å ha loggmateriale tilstrekkelig tilbake i tid slik at etterforskning og effektiv feilretting blir mulig. Logger fra nettverksutstyr, webservere, brannmurer og påloggingstjenester er nettverkets "overvåkningskamera", og et relativt rimelig sikringstiltak.

Gode rutiner rundt logging kan avdekke kvalitetsproblemer og om utstyr er i ferd med å gå i stykker (eksempelvis disker og annet utstyr som potensielt påfører virksomheten nedetid og produksjonstap). Man kan unngå kapasitetsproblemer ved å oppgradere i tide. Det er i mange tilfeller et nødvendig virkemiddel for å oppnå samsvar med lovverk og kommersielle regelverk. Logganalyse gir kunnskap om trafikk og uønsket aktivitet og er et nyttig virkemiddel til å forstå eget driftsmiljø og teknologi. Også etter et angrep, eller normalstilling etter en driftsfeil, er logger en nyttig kilde for kunnskap om at problemet virkelig er løst.

Sist, men ikke minst, skal man ha noe nytte av loggene sine er det viktig å ta disse i bruk, og se på dem som en ressurs for forbedret og sikrere drift.

Oppdagelsesevne

Egne ansatte og oppfølging av alarmer og logger anses av virksomhetene som de viktigste kildene til å oppdage hendelser. De store virksomhetene har større oppmerksomhet på signaler fra ansatte, og på analyser fra systemer og logger som er på plass for å detektere trusler. Samtidig er trenden nedadgående for hendelser som er oppdaget av eksterne leverandører som ISP, politiet og andre samarbeidspartnere.

Hva er dine viktigste kilder til å oppdage sikkerhetshendelser i egen virksomhet?	Under 10 ansatte	10 til 99 ansatte	100 ansatte eller flere	Total
Rapportering/varsling fra egne ansatte	53 %	66 %	80 %	70 %
Media (radio, TV, aviser), sosiale medier	14 %	15 %	16 %	15 %
Egen oppfølging av alarmer, logging og IDS-systemer	26 %	35 %	66 %	48 %
Eksterne (eks. Internet Service Provider, Politi)	9 %	15 %	29 %	21 %

Fortsettelse fra s 26: **Hva er dine viktigste kilder til å oppdage sikkerhetshendelser i egen virksomhet?**	**Under 10 ansatte**	**10 til 99 ansatte**	**100 ansatte eller flere**	**Total**
Annet	4 %	7 %	7 %	6 %
Vet ikke	28 %	17 %	4 %	13 %

Anbefaling

- Sørg for jevnlig opplæring av ansatte i informasjonssikkerhet. Dette hjelper både for å hindre hendelser og for å oppdage hendelser. Jevnlig fokus på farene ved virus, phishing og sosial manipulering gir stor uttelling. Sørg også for at nyansatte alltid får en sikkerhetsgjennomgang.
- Ha rutiner og automatikk for systematisk å gjennomgå logger, avvik og varsler, eksempelvis fra antivirussystemene. Dette kan enten gjøres internt, hos ekstern sikkerhetsleverandør, eller at tjenesteleverandøren gjør dette i deres systemer.
- Ha overvåkningssystemer for oppdagelse av sikkerhetshendelser, IDS.

Med støtte fra:

buypass securing transactions

mnemonic - securing your business

telenor