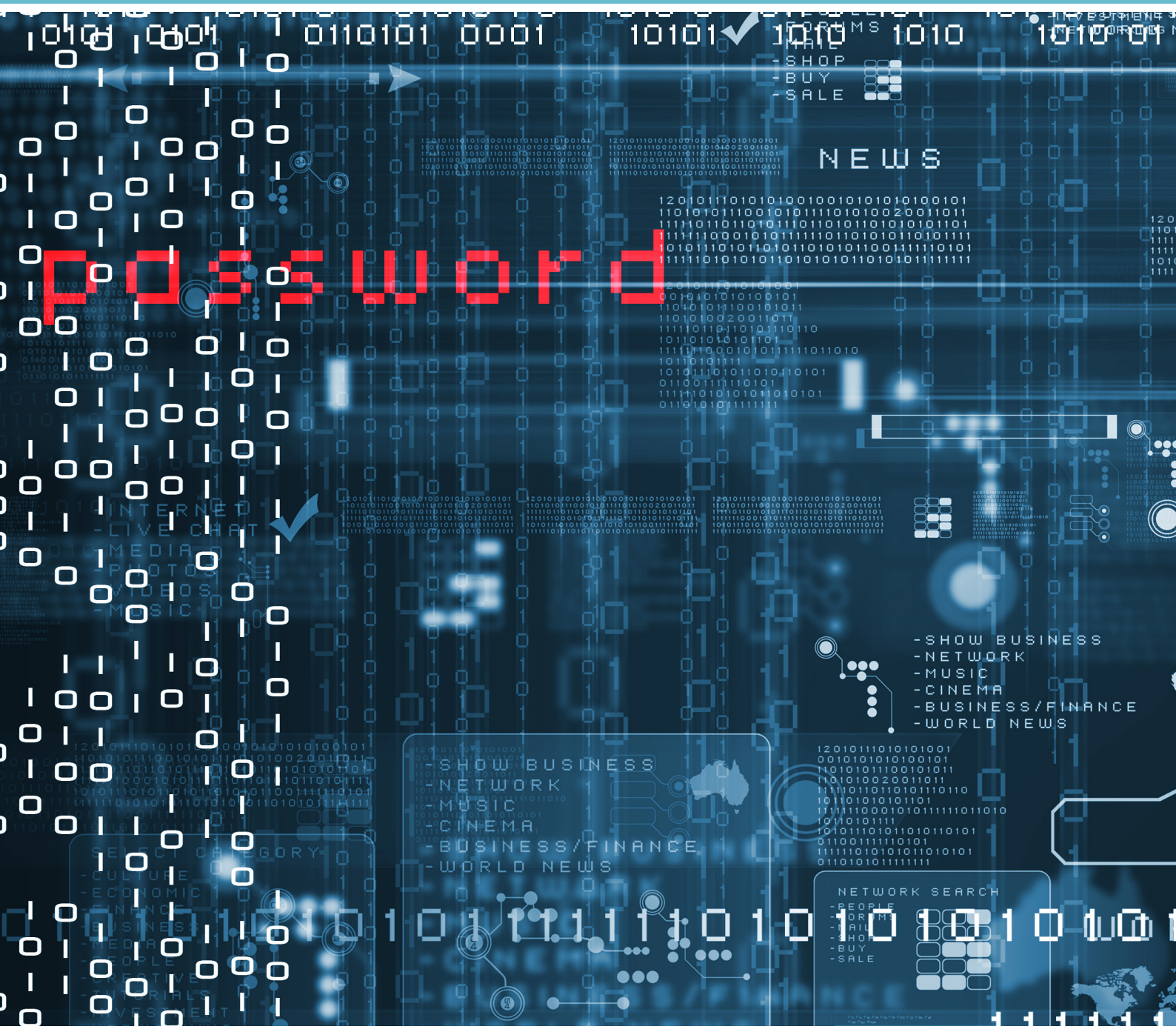
MØRKETALLSUNDERSØKELSEN 2016

- Informasjonssikkerhet, personvern og datakriminalitet



NSR NÆRINGSLIVETS SIKKERHETSRÅD

INNHOLD

Publisert:
september 2016

Trykk:
NHO Servicepartner

Layout og illustrasjoner:
Næringslivets Sikkerhetsråd

Foto:
Adobe Stock

Kontakt:
E-post: nsr@nsr-org.no

Adresse:
Middelthuns gate 27, Majorstuen

1 INNLEDNING

Hovedbudskap

Over en fjerdedel av norske virksomheter – 412 av 1500, eller 27% – har opplevd uønskede sikkerhetshendelser det siste året. Virksomhetene forteller at dette fører til produktivitetstap i 4 av 10 tilfeller (i form av tapte arbeidstimer), men kun 2 av 10 oppgir at de har hatt kostnader som følge av slike hendelser. Dette viser at virksomhetene mangler oversikt over hva sikkerhetshendelsene koster dem, eller undervurderer disse kostnadene. Kun 9% av virksomhetene som utsettes for angrep tar saken videre til politiet. Det tilsier at det skjuler seg betydelige mørketall, og for de kriminelle nettverk er denne typen angrep mot norske virksomheter i praksis straffefrie.

Datagrunnlaget

For Mørketallsundersøkelsen 2016, som er den 10. undersøkelsen gjennomført av NSR, ble totalt 1500 virksomheter intervjuet av Opinion per telefon i perioden 18.mai til 9.juni 2016. Opinion kontaktet et tilfeldig utvalg virksomheter fra foretaksregisteret med fem eller flere ansatte, hvilket førte til at respondentene i årets undersøkelse gjenspeiler den generelle næringsstrukturen i Norge i større grad enn tidligere. Hovedvekten av virksomhetene er små, og andelen store er betydelig mindre enn i tidligere undersøkelser. Ny innsamlingsmetode gjør det vanskelig å sammenligne data over tid, og derfor sammenlignes ikke årets funn med tidligere undersøkelser. Årets undersøkelse er inspirert av en undersøkelse gjennomført i Storbritannia[1] , og fokuset er på oppdagelse og håndtering av hendelser, med utgangspunkt i den verste hendelsen.

1 http://www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-digital.pdf

Informasjonssikkerhetsutvalget har bestått av:

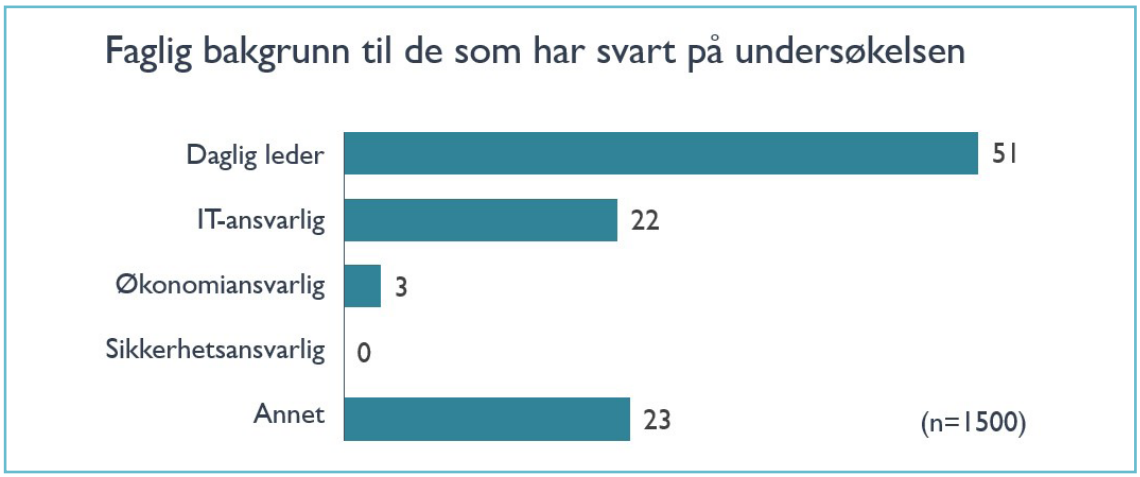
- Tønnes Ingebrigtsen (mnemonic, leder)
- Janne Hagen (Norges vassdrags- og energidirektorat)
- Vidar Østmo (Verdipapirsentralen)
- Johnny Mathisen (Telenor)
- Ole Tom Seierstad (Microsoft)
- Christophe Birkeland (Blue Coat Norway)
- Eiliv Ofigsbø (Kripos)
- Martha Eike (Datatilsynet)
- Bente Hoff (Nasjonal Sikkerhetsmyndighet)
- Roger Johnsen (Norsk senter for informasjonssikring)
- John Arild A. Johansen (Helsedirektoratet)
- Arne Røed Simonsen (NSR)

- Fredrik Walløe (mnemonic, skribent)

2 MER OM UNDERSØKELSEN

Hvem svarte?

I over halvparten av svarene var respondenten daglig leder, mens 22 % av dem hadde bakgrunn som IT-ansvarlig. Merk at i mange mindre og mellomstore virksomheter har IT-ansvarlig også rollen som sikkerhetsansvarlig. De resterende 27% hadde en annen (og variert) bakgrunn.



Virksomhetene som svarte på undersøkelsen har i gjennomsnitt 39 ansatte. Det er kun 89 virksomheter med flere enn 100 ansatte blant de 1500 i datasettet.

Majoriteten av virksomhetene tilhører følgende bransjer:

- Varehandel og reparasjon av motorvogner 21%
- Undervisning 18%
- Helse- og sosialtjenester 18%

Det er verdt å merke seg at det bare er de innledende spørsmålene som har 1500 respondenter. For resten av spørsmålene, der vi spør om forhold rundt den verste hendelsen, er datagrunnlaget begrenset til de 412 respondentene som har opplevd uønskede hendelser.

Organisering av IT-driften

Av 1500 virksomheter som svarte på spørsmålet om hvordan deres IT-drift er organisert, oppga 44% at de selv drifter sine egne systemer, 22% setter ut driften (outsourcer) helt mens 31% velger en mellomløsning.

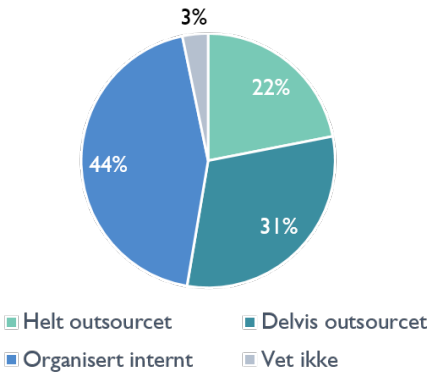
Av de 790 virksomhetene som svarte på spørsmålet om de benytter outsourcingstjenester i utlandet svarer kun 8% at de gjør dette.

Hele 86% sier de vet hvor deres data er lagret, mens 14% ikke vet.

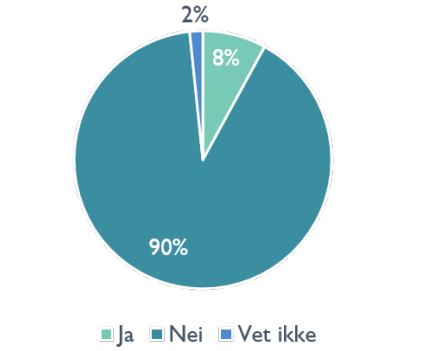
Rammeverk og/eller styringssystem for informasjonssikkerhet

Av 1500 svarer 60% at de har et styringssystem for informasjonssikkerhet.

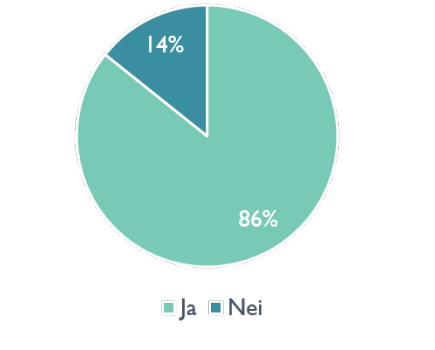
Organisering av IT-driften



Outsourcingstjenester i utlandet



Kunnskap om hvor data er lagret



3 RISIKOBILDET

Risikobildet fra NSM

NSM NorCERT har som oppdrag å detektere, varsle og bistå ved hendelseshåndtering i forbindelse med angrep mot samfunnskritisk infrastruktur eller samfunnsviktige funksjoner. Innenfor rammen av dette oppdraget har NSM NorCERT gjennom flere år sett en tydelig og jevn økning av antall målrettede IKT-angrep mot norske interesser, både offentlig og privat. I tillegg til en økning av målrettede angrep er det et stadig økende omfang av ulike politiske og kriminelt motiverte handlinger i det norske cyberdomenet.

Alvorlige målrettede angrep

I 2015 registrerte NSM NorCERT et trendbrudd, og antallet detekterte alvorlige angrep mot samfunnskritisk infrastruktur eller samfunnsviktige funksjoner var lavere enn i 2014. Årsaken til dette er sammensatt, men NSM NorCERT mener det skyldes at en andel av angrepene har blitt mer avanserte. Basert på tallene fra NSM NorCERT kan det ikke trekkes bastante konklusjoner om det faktiske antallet målrettede angrep og trusselaktører er økende, eller om de eksisterende aktørene har gjennomført flere angrep sammenlignet med tidligere. Angrepene er imidlertid vedvarende og viser at trusselaktørene har ressurser til metodisk aktivitet over lengre tid.

Fellestrekk fra det totale antallet vellykkede angrep er at hovedangrepsvektor i målrettede angrep er epost til brukere i målorganisasjonen. Eposten inneholder et ondsinnet vedlegg eller en link til en side som inneholder ondsinnet kode. I de fleste tilfeller er eposten utformet med relevant informasjon for mottakeren og sendes kun til et fåtall utvalgte brukere (spearphishing). Informasjonen om epostmottakeren blir hentet ut fra informasjon som angriper har tilgang til, enten fra åpne kilder eller tidligere kompromittert informasjon.

Dessverre ser NSM NorCERT at angrep som benytter eldre sårbarheter fortsatt lykkes. Det er kun unntaksvis at «ikke kjente sårbarheter», såkalte 0-dags sårbarheter, blir utnyttet. Det siste året har NSM NorCERT vært involvert i mange saker der utdaterte webserverinstallasjoner hos mindre bedrifter med begrensede IT-ressurser har blitt kompromittert. De kompromitterte serverne blir så brukt som mellomledd i nye angrep mot andre mål, både nasjonalt og internasjonalt.

Hacktivisme i Norge

Hacktivisme er en aktivitet som i hovedsak benytter datamaskiner og nettverk til å fremme et standpunkt eller en politisk agenda. Ofte ser man bruk av sosiale medier som Twitter for å fremme en kampanje, der man for eksempel oppfordrer til boikott av eller angrep på en eller flere virksomheter. Angrepsmetoder og konsekvenser i slike angrep varierer kraftig.

Internasjonalt er DDoS mye brukt, da konsekvensen ofte er synlig og får lett medieomtale av typen "hacker tok ned tjeneste X". DDoS er også lett og billig å gjennomføre.

En annen angrepsmetode er å endre innholdet på nettsiden til offeret. Det er også blitt mer vanlig å publisere sensitivt materiale på nett, som igjen kan skade omdømmet til virksomheten.

Selv om hacktivisme har et lite omfang i Norge ser NSM NorCERT en økende tendens de siste årene. I 2015 og 2016 kjørte Anonymous en kampanje mot hvalfangst, hvor Norge, Island og Japan ble satt på angrepslisten. Under emnetagger som #OPSEAWORLD, #OPKILLINGBAY og #OPWHALES på Twitter, oppfordret man til boikott av Norge. Kampanjen toppet seg tidlig i 2016 da flere norske nettsider delvis ble tatt ned. Angrepet tvang hostingleverandørene til å blokkere trafikk fra utlandet for å holde nettsidene oppe.

Det kan være vanskelig å bedømme om et DDoS-angrep er knyttet til hacktivisme, utpressing eller er et målrettet angrep da det ikke alltid er enkelt å knytte et DDoS-angrep til en spesifikk hacktivistkampanje. Hittil i 2016 har NSM NorCERT observert 13 DDoS-angrep, mot 10 i 2015. 40% kan knyttes til hacktivisme.

NSM NorCERT har ikke observert noen angrep utført av hacktivister som har fått store samfunnsmessige konsekvenser i Norge så langt, men lengre nedetid på tjenester og nettsider har forekommet. Dette kan imidlertid endre seg. Av andre risikomomenter er tyveri og publisering av sensitive opplysninger kanskje en av de større risikofaktorene som norske virksomheter bør ta høyde for i tillegg til DDoS-angrep.

Det vil i tiden fremover være viktig å ikke undervurdere hacktivistgruppene og deres evne til å gjennomføre betydelige angrep.

Cyberkriminalitet i Norge

Det siste året har det vært en kraftig oppgang i utsending av løsepengevirus på epost. NSM NorCERT og andre sektorCERTer har samarbeidet ved flere tilfeller der det har vært varslet angrepsbølger. Selv om ulike nasjonale og internasjonale sikkerhetsmiljøer arbeider hardt med å ta ned infrastrukturen som blir benyttet i angrepene, er det likevel mange - både privatpersoner og virksomheter - som blir rammet. Varsler sendt ut av NSM NorCERT i 2015 har hatt fokus på viktigheten av å ha gode rutiner for sikkerhetskopiering. Det finnes mange konkrete eksempler på angrep med løsepengevirus hvor det har vært svært vanskelig å rekonstruere filene når de først er kryptert. Noe av grunnen til at angrepene har vært vellykket i Norge er utformingen av eposten der angriper utgir seg for å være fra Posten eller en annen norsk virksomhet. At eposten også er skrevet på god norsk bidrar til at mange lar seg lure. NSM NorCERT har anbefalt å ikke betale løsepengene. Dette fordi man ikke har noen garanti for at man faktisk vil motta en korrekt nøkkel, samt at dette oppfordrer angriper til å fortsette med utpressingskampanjer.

NSM NorCERT har observert at det hele tiden kommer nye krypteringsvirus på markedet, og såkalt ransomware-as-a-service gjør det svært lett å sende ut slik epost. Så lenge folk velger å betale, kan man anta at denne type aktivitet vil fortsette å øke. NSM NorCERT får daglig rapporter fra samarbeidspartnere om kompromitterte norske nettsider som omdirigerer til nettsider som er infisert av skadevare (Exploit Kits). Dette har vært en vanlig angrepsvektor for distribusjon av krypteringsvirus, men også andre typer skadevare har vært distribuert.

I slutten av 2015 var det mye fokus rundt gruppen DD4BC (DDoS for bitcoins) og Armada Collective. Disse grupperingene spesialiserte seg på utpressing av bedrifter med trusler om et stort DDoS-angrep hvis man ikke betalte en sum Bitcoins. Gruppen opplevde relativt stor suksess da beløpene de krevde ofte var såpass lave at en større virksomhet vurderte det som lettest å bare betale. Etter en større internasjonal politiaksjon ble flere av bakmennene bak DD4BC arrestert, og man opplevde stor effekt. I ettertid observerte NSM NorCERT en rekke copy-cats som forsøkte samme strategi, men uten en faktisk DDoS-kapasitet uteble suksessen.

Direktørsvindel

Phishing og falske faktura er intet nytt, men en ny trend i 2016 er såkalt direktørsvindel, også kalt whaling. Essensen i slike angrep er at man på forhånd gjør undersøkelser av virksomheten man ønsker å angripe. Man kartlegger økonomisjefer eller ansatte med ansvar for transaksjoner i en virksomhet. Angrepet starter ofte med en epost med forfalsket avsender. Dette kan gjøres ved å utnytte svakheter i hvordan avsender vises i epostprogrammer, eller ved såkalt typosquatting (et eksempel er @bedrift.com versus @bedrif.com), der man registrerer et domene som til forveksling ligner på bedriftens domene. Epostene er ofte skrevet på godt norsk, og man blir bedt om å gjennomføre en hastebetaling som må holdes hemmelig. Ofte starter korrespondansen med en epost som sier «Hei, er du på kontoret? Mvh Sjef». Deretter vil en falsk faktura bli oversendt med et innhold som passer inn med det virksomheten driver med. Denne sosiale manipulasjonen har vist seg å være svært effektiv, og NSM NorCERT har informasjon om at flere norske virksomheter har betalt relativt store summer til utlandet. NSM NorCERT har et godt samarbeid med FinansCERT og bankene som fortløpende svartelister bankkonti og etterforsker videre. NSM NorCERT sendte flere varsler i samarbeid med HelseCERT der vi ønsket å rette oppmerksomheten mot slike eposter. I perioden juni til august 2016 har NSM NorCERT blitt varslet av 45 virksomheter som hadde blitt utsatt for direktørsvindel. Flere av disse ser ut til å ha blitt forsøkt lurt av flere forskjellige aktører. Basert på infrastruktur observert i angrepene er antallet bedrifter som varsler NorCERT om denne typen hendelser minimal, og det er derfor store mørketall.

I 2016 har trenden fortsatt gjennom andre former for generisk svindel der man misbruker kjente merkevarenavn som Netflix, Amazon og PayPal. Såkalt "Microsoft Callsender Fraud" der angriper ofte ringer offeret og sier at datamaskinen er infisert er fortsatt et problem. Det er også observert tilfeller der svindlere utgir seg for å komme fra Nasjonal Sikkerhetsmyndighet. Det ble i 2016 skrevet mye om dette i media, noe som bidrar til økt og viktig bevisstgjøring.

Trusselvurdering fra mnemonic

Introduksjon

mnemonics kunder representerer alle typer virksomheter – offentlige så vel som private. Totalt dekker mnemonics sikkerhetsmonitoreringstjenester flere hundre tusen arbeidstakere, hvorav flesteparten av disse befinner seg i Norge. Siden deres trusselvurdering for Mørketallsundersøkelsen 2014 har mnemonic varslet sine kunder om over 35 000 sikkerhetshendelser. Hele 9 av 10 har blitt kompromittert av skadelig kode.

IT- og informasjonssikkerhetsutfordringene Norge står overfor har aldri vært større. mnemonic mener det er avgjørende at sikkerhetsbransjen tar et oppgjør med unødvendig hemmelighold. Gradering av informasjon om trusler og angrep må balanseres med delingsbehovet. Hypotesen deres er at dersom det norske IT-sikkerhetsmiljøet visste hva hele miljøet samlet vet kunne langt flere angrep vært forhindret. Det har skjedd store fremskritt på dette området de siste to årene, men vi har fortsatt en lang vei å gå.

I deres trusselvurdering for 2016 ønsker mnemonic å fokusere på tre primære trusselagenter; organisert kriminalitet, aktivisme og etterretning.

Organisert kriminalitet

Den 18. april 2016 kunne VG fortelle om norgeshistoriens sannsynligvis største ran. Ved å utgi seg for å være toppsjefen i et internasjonalt selskap vant ranere tilliten til medarbeiderne hos en norsk virksomhet. I løpet av få dager var en halv milliard kroner på avveie. Svindelen ble oppdaget, transaksjoner ble stanset, og kontoer fryst. Likevel sitter de kriminelle igjen med anslagsvis 100 millioner kroner. Til sammenlikning kom NOKAS-ranerne seg unna med drøyt halvparten. Likevel hører man lite om sjokkbrekket i media. Noen vil kanskje påstå det var mindre alvorlig siden ingen ble såret eller drept. I motsetning til tradisjonelle brekk ble det hverken benyttet våpen, masker eller fluktkjøretøy. Ranet skjedde på internett.

Det føderale politiet i USA har i tidsrommet oktober 2013 til februar 2016 registrert 17.642 ofre for såkalt direktørsvindel, med et samlet tap på 2,3 milliarder amerikanske dollar. Statistikken i Norge er mangelfull, men mnemonic er kjent med at flere norske virksomheter er rammet i ulikt omfang. Listen over ofre vokser, men mørketallene er store, og mange vegrer seg av ulike årsaker for å anmelde hendelsene.

Den mest signifikante utviklingen mnemonic har observert i løpet av de siste par årene er bruken av utpressing. Hittil har slike angrep i hovedsak rammet opportunistisk; intetanende brukere åpner innhold i e-poster fra ukjente avsendere - for eksempel hentelapper fra Posten, eller surfer på nettsider som serverer skadevoldende kode. Mange har måttet krype til korset ved å betale løsepenger for å låse opp krypterte data man ikke har råd til å miste.

Samtidig er mnemonic mer bekymret for datainnbrudd hvor ofrene ikke er tilfeldig valgt. Det er sannsynligvis bare et tidsspørsmål før vi opplever målrettede angrep som holder samfunnskritiske virksomheters informasjonsaktiva som gissel. Verre blir det når disse virksomhetene av ulike årsaker ikke har råd til å unnlate å betale. I USA har eksempelvis sykehus gitt etter for denne typen utpressing. De kriminelle grupperingene som utvikler og sprer skadevare har alle fordelene, mens både offentlige og private norske virksomheter samt privatpersoner forsvarer seg med bind for øynene og en hånd bundet bak ryggen.

Dessverre finnes det ingen enkle løsninger på sikkerhetsutfordringene digitaliseringen av Norge medfører. Det vi derimot vet er at både forbrukere og myndigheter har mye å hente ved å stille krav til sikkerheten i løsningene man velger å benytte seg av. I tillegg er det på tide å begrave tabuet forbundet med å bli "hacket". En høynet bevissthet om hva dagens datakriminelle er i stand til å gjøre vil i seg selv kunne virke forebyggende. Dersom flere hadde stått frem på lik linje med eksempelvis Telenor, Ulstein Group og Lånekassen, ville andre innbrudd kanskje vært unngått.

Myndighetene har begynt å ta tak i utfordringene, rapporten fra Lysneutvalget, senere års funn fra Riksrevisjonen, råd fra Nasjonal sikkerhetsmyndighet og Justisdepartementets (JD) "Datakrimstrategi" inneholder alle konkrete tiltak som kan bedre sikkerheten, bekjempe datakriminalitet og styrke personvernet. Tiden vil vise om tiltakene lar seg gjennomføre.

Hacktivisme

I løpet av det siste tiåret har vi blitt kjent med en ny variant av politisk aktivisme. Hacktivisme, et teleskopord bestående av hacking og aktivisme, beskriver utnyttelsen av IT-systemer for å påvirke holdninger i samfunnet, samt å spre ideologisk og politisk propaganda.

De norske hacktivistmiljøene fremstår som fragmenterte. Oppslutningen vurderes som lav, og ledelsesvakuumet gjør det utfordrende å koordinere med likesinnede.

Samtidig kan slike miljøer utgjøre en moderat trussel. Sommeren 2014 gjennomførte en tenåring omfattende tjenestenektangrep mot flere av landets største virksomheter, og i 2016 ble både Miljøpartiet de Grønne (MDG) og Sosialistisk Venstreparti (SV) utsatt for innbrudd som blant annet førte til at partienes medlemslister både ble manipulert og havnet på avveie. Selv om angrepene ble utført av enkeltpersoner inneholder de et viktig budskap; tilgangen på kunnskap og ressurser som kreves for å gjennomføre angrep blir stadig bedre, og verktøyene blir enklere i bruk. Denne utviklingen vil sannsynligvis senke terskelen for å delta, samt øke rekrutteringsmulighetene. I kombinasjon med manglende ledelsesstruktur i hacktivistmiljøene gir dette grunnlag for bekymring. Den gjennomsnittlige hacktivisten er en ung mann, som sannsynligvis vil kunne la seg påvirke av mer erfarne "kollegaer". Det er derfor mulig at mer ressurssterke grupper med andre motiver kan misbruke hacktivistene som et ledd i å oppnå sine mål.

Etterretning

Etterretning kan defineres på flere måter, men kan i grove trekk forklares som de aktiviteter, prosesser og produkter som reduserer usikkerhet og bidrar til å skape operasjonelle- eller konkurransefordeler.

Den teknologiske utviklingen i samfunnet, især bruken av internett, gjør oss stadig mer sårbare, og trusselen mot norske interesser varierer fra virksomhet til virksomhet. Fremmede staters etterretningsvirksomhet vil også være ulik, avhengig av hva de ønsker å oppnå.

Etterretningstjenestens årlige ugraderte vurdering av aktuelle sikkerhetsutfordringer - FOKUS 2016 - navngir både Russland og Kina som fremmede stater som har gjennomført "vedvarende aktiviteter mot norske myndigheter og virksomheter". Det er verdt å poengtere at Norge er et av få vestlige land som retter pekefingeren mot spesifikke fremmede staters etterretningsaktiviteter i offisielle og ugraderte rapporter.

Etterretningstjenesten deler trusler i det digitale rom i tre kategorier: etterretning, sabotasje og påvirkning, noe også mnemonic mener er hensiktsmessig. Felles for disse kategoriene er trusselaktørenes behov for å unngå å bli identifisert. Fremmede staters etterretningstjenester vil i de fleste tilfeller dra nytte av ikke å bli ansvarliggjort for angrep eller innbrudd. I mange tilfeller vil de også strekke seg langt for å kunne benekte sin involvering, eller så tvil om årsaken til hendelsen. Ressursene slike tjenester rår over betyr i praksis at det er svært utfordrende å sikre seg, selv for modne organisasjoner med solide forsvarsmekanismer og sikkerhetsfokus.

Spionasje

I løpet av de senere årene har mnemonic gransket flere alvorlige hendelser hvor de aktuelle trusselaktørene har benyttet seg av svakheter hos tredjepartsleverandører som et vesentlig ledd i angrepene på deres endelige mål. Etterhvert som bruken av skylagring og skytjenester øker vil ressurssterke aktører i mindre grad ha behov for å bryte seg inn direkte hos den aktuelle virksomheten. Tjenesteutsetting kan ha mange fordeler, også sikkerhetsmessige, men disse bør veies opp mot sikringsbehovet.

Sabotasje

Sabotasje som et direkte, tiltenkt resultat av datainnbrudd fikk først oppmerksomhet når Stuxnet-ormen ble oppdaget i 2010. Angrepet på Irans atomprogram gjenåpnet debatten om sårbarheter i kritisk infrastruktur, og mange forventet at vi ville se flere lignende angrep. Med unntak av et angrep mot et tysk industrianlegg i 2014 kunne det virke som om dommedagsprofetiene ikke ennå hadde gått i oppfyllelse. Julen 2015 forandret dette seg da et koordinert angrep mot kraftnettet i den ukrainske regionen Ivano-Frankivsk førte til at over hundre tusen hjem mistet strømtilførselen. Offentlig tilgjengelige analyser viser at angriperen etter å ha låst operatørene ute av systemet skrudde av sikringer som førte til at nærmere 30 trafostasjoner gikk av nett. Samtidig slo de til mot to hovedtrafoer og saboterte nødstrømsløsningene, noe som førte til at både omfordeling av strøm og feilretting tok lengre tid enn estimert. Hendelsen illustrerer at selve bærebjelken i det digitaliserte samfunnet, tilgangen på strøm, er sårbar nok til å la seg sabotere av ressurssterke aktører. For norske virksomheter betyr denne utviklingen at man i langt større grad enn før må ta høyde for at tradisjonelle beredskapstiltak ikke alltid vil være til å stole på, noe som stiller svært høye krav til redundans og motstandsdyktighet.

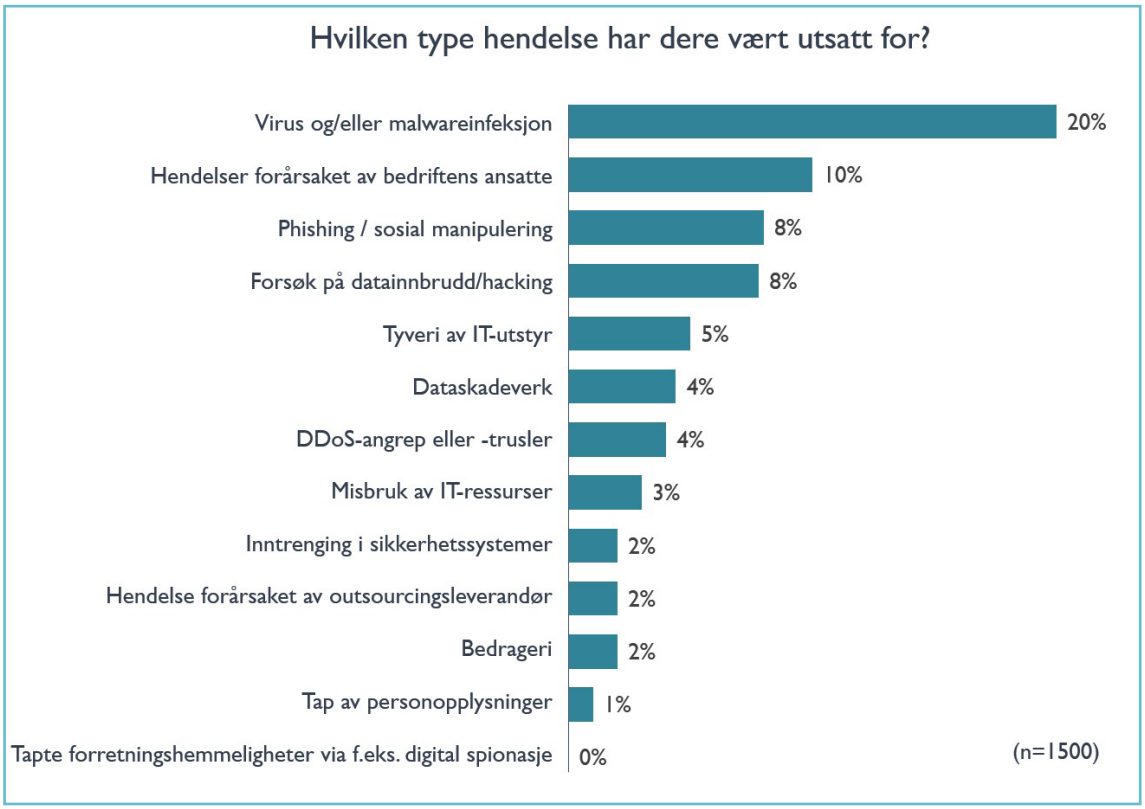
Påvirkning

Påvirkning handler om å misbruke nyhetskilder og sosiale medier i den hensikt å manipulere informasjonsmottakerens virkelighetsoppfatning. Ikke overraskende er det få vellykkede angrep av denne typen som blir kjent. I 2016 har det derimot blitt lekket sensitiv informasjon fra det amerikanske demokratiske partiet. Det er foreløpig uvisst hvem som står bak angrepet, men flere eksperter peker på Russland. Hvis dette er tilfellet utgjør hendelsen et vannskille, en fremmed stat kan ha gjennomført datainnbrudd i den hensikt å påvirke det amerikanske presidentvalget. Sett fra et norsk perspektiv kan man forestille seg mange økonomiske og politiske temaer hvor flere aktører sannsynligvis vil forsøke å utøve sin innflytelse; Storbritannias valg om å melde seg ut av EU, økt innvandring som følge av uro i Midt-Østen, og et stadig kaldere sikkerhetspolitisk klima grunnet Russlands stormaktsambisjoner. 11. september 2017 er det også Stortingsvalg i Norge. Det er ikke usannsynlig at fremmede stater vil være interessert i å påvirke opinionen.

4 DATAINNBRUDD OG SIKKERHETSHENDELSER

Virus og skadevare rammet minst en av fem virksomheter i 2015. Denne brede kategorien inkluderer alt fra skadevare som sluker dataressurser og skaper irritasjon, til alvorlige infeksjoner som kan føre til omfattende tap av filer, tyveri av intellektuell eiendomsrett og stopp i arbeidet. Av de 1500 virksomhetene som svarte på spørsmålet om sikkerhetshendelser var det også 10% som rapporterte om hendelser forårsaket av virksomhetens ansatte. Deretter følger sosial manipulering og forsøk på datainnbrudd, som begge er på 8%.

Kun 4% av de 1500 virksomhetene opplevede distribuert tjenestenekt (DDoS). Det var ingen betydelige forskjeller mellom hvilke bransjer disse tilhørte, men små virksomheter er i langt mindre grad offer for slike angrep enn store virksomheter. I gruppen 5-19 ansatte er det 3% som har rapportert DDoS, i gruppen 20-99 ansatte er det 4% som rapporterer at de har hatt DDoS-hendelser, mens i gruppen store virksomheter (100 ansatte eller flere) er det 12% som har opplevd DDoS-angrep.



Avdekkede hendelser fra Telenor

DDoS

Telenor har utstyr plassert i eget kjernenett for å oppdage og filtrere DDoS-angrep, samt en tjeneste for bedriftskunder der angrep blir aktivt filtrert etter hvert som de blir oppdaget.

I det siste året har det vært i gjennomsnitt 750 angrep i måneden mot Telenors nett og kunder i Norge, Sverige og Danmark. Dette tallet har holdt seg ganske jevnt det siste året. I det siste halvåret har det imidlertid vært to måneder som har skilt seg ut med rekordstore enkelt-angrep. Disse kom i april og juni med henholdsvis 163Gbps og 277Gbps. Det kreves solid infrastruktur for å klare å motstå denne typen angrep.

Når det gjelder angrep mot Telenors bedriftskunder ser vi at et typisk angrep varer i 30 minutter og er på 6Gbps. I løpet av en måned blir disse kundene utsatt for mellom 5 og 20 angrep.

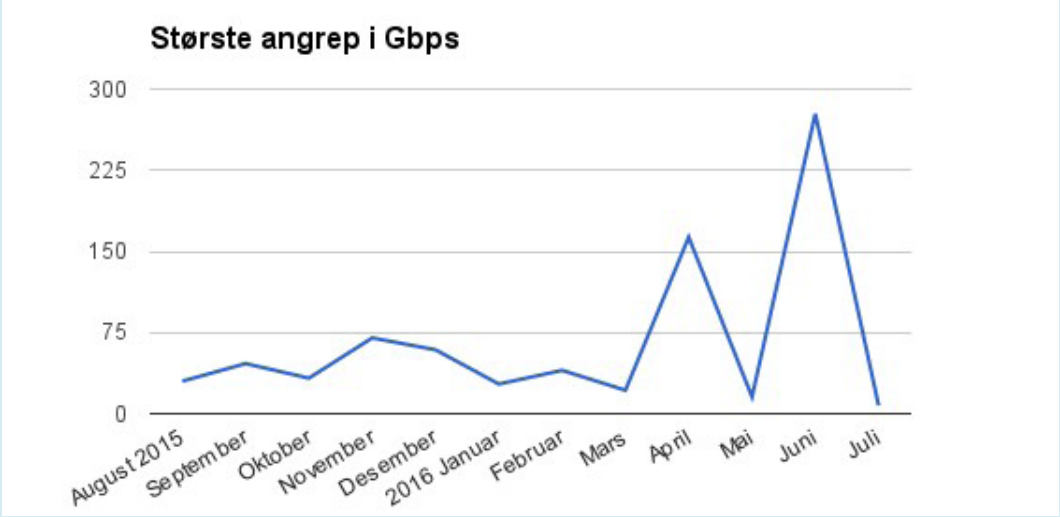
Angrepene består fortsatt for det meste av reflekterte pakker. Angriperne sender ut store mengder spoofede pakker (forfalsket avsender-adresse) til tusenvis av feilkonfigurerte servere på Internett. Serverne sender så svaret tilbake igjen til offeret. Dette gjør at angriperne kan sende ut relativt få pakker og få forsterket angrepets størrelse flere titalls ganger. Det er gjerne servere som kjører NTP (Network Time Protocol), DNS (Domain Name System) og CHARGEN som blir misbrukt.

I de siste månedene har Telenor også sett et oppsving i direkte angrep ved hjelp av store mengder SYN-pakker. SYN-pakker brukes til opprettelse av en Internett-forbindelse. Disse pakkene kan ikke forsterkes ved hjelp av refleksjons-angrep, så de sendes direkte fra kompromitterte servere med høy båndbredde eller fra botnet for å overbelaste tjenesten.

De fleste DDoS-angrep blir raskt filtrert, og angrepet bekjempes i løpet av noen minutter. Telenor har imidlertid sett eksempler på mer avanserte angrep, der angriperne tydelig har gjort forarbeide. I noen tilfeller er det tydelig at angriperne følger med på responstiden til tjenesten de angriper, og endrer angrepstypen hvis de ser at angrepet ikke lykkes eller blir avverget. Telenor har også sett angrep der samme kunde blir angrepet flere steder samtidig, f.eks. på tjenester som leveres fra ulike datasentre. Denne typen angrep er ikke tilfeldig og utføres gjerne av en konkurrent eller noen som driver med utpressing.

Sikkerhetsovervåking

Telenor Security Operation senter (TSOC) har en tjeneste for sikkerhetsovervåking av kunders nettverk. En sensor blir plassert i kundens nettverk for å overvåke trafikken og se etter uønsket trafikk og infiserte maskiner. I løpet av de siste tre årene har Telenor sett noe nedgang når det gjelder alvorlige uønskede hendelser hos sine kunder. Allikevel har mer enn 85% av TSOCs kunder blitt utsatt for en alvorlig uønsket hendelse i løpet av de siste to årene.



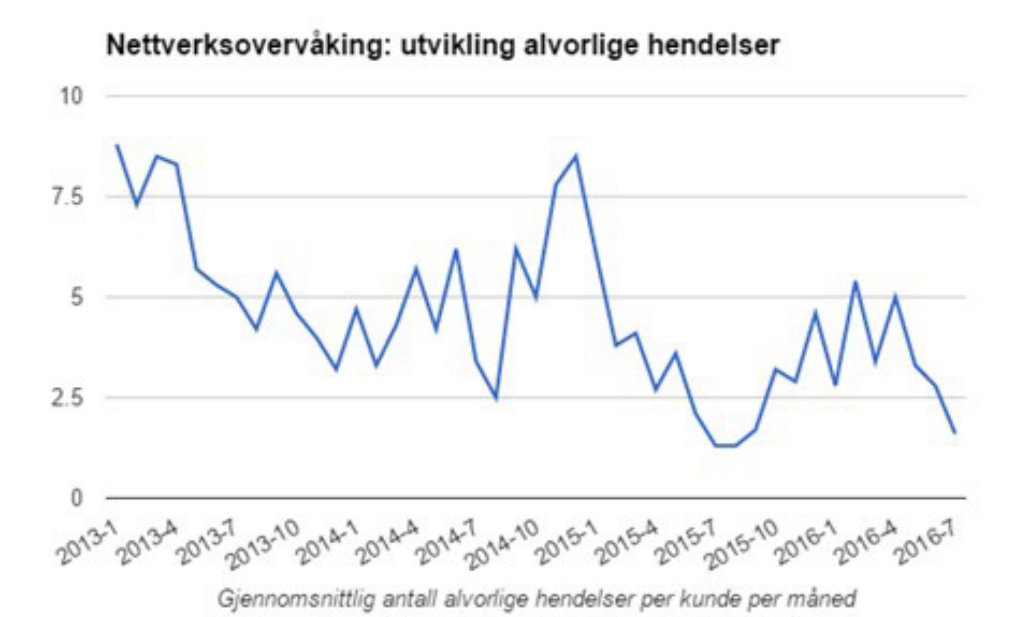
For et par år siden ble mange maskiner kompromittert ved hjelp av såkalte "drive-by-exploits", altså at maskinen blir infisert av skadevare kun ved at brukeren besøkte en nettside. Ofte var det tredjeparts plugins til nettlesere som hadde svakhetene som ble utnyttet, f.eks Java, Silverlight og Flash. Som et motsvar til dette begynte mange nettlesere å blokkere sårbare plugins. Nettlesere ble etter hvert også oppdatert automatisk og stadig hyppigere. Dette har ført til at det er færre svakheter som er lette å utnytte på de fleste bedrifts-PCer.

Det har i det siste fortsatt vært en dreining mot mer bruk av sosial manipulasjon, der brukere blir lurt til å installere skadevaren selv eller til å gi fra seg sensitiv informasjon, såkalt phishing. Inngangsporten til dette er gjerne vedlegg i e-poster som pirrer nysgjerrigheten til brukeren, skremmende/truende annonser på web eller at skadevare lurer seg inn på maskinen som vedlegg til mer eller mindre kjente programmet som brukeren installerer.

Før sommeren i 2016 var det en større bølge av ransomware mot bedrifter i Norge der mange bedrifter opplevde å få kryptert både enkeltmaskiner og filservere. Skadevaren ble gjerne spredd som vedlegg til e-poster. Telenor har inntrykk av at mange bedrifter nå har satt på bedre filtrering av vedlegg i e-poster, noe som har bidratt til å begrense spredningen i det siste. I USA har det også vært tilfeller av målrettede ransomware-angrep mot bedrifter, da spesielt sykehus. Angripere kommer seg inn i nettverket, krypterer mange kritiske servere samtidig og krever store summer i løsepenger. Dette har Telenor ikke sett mye til i Norge så langt.

I 2016 har det også vært en sterk økning i såkalt direktørsvindel eller CEO-svindel. Denne svindelen går ut på å sende forfalskede e-poster til ansatte som kan utføre betalinger til utlandet. E-postene ser gjerne ut til å komme fra firmaets administrerende direktør. Dette er en type svindel som kan være vanskelig å stoppe med tekniske sikkerhetstiltak. Her må en sørge for gode rutiner rundt betalinger, samt opplæring av medarbeidere.

Flere maskiner får også installert programmer som er i grenselandet av det som er ønskelig og lovlig, såkalte "potentially unwanted programs". Disse programmene blir gjerne installert sammen med annen programvare som brukere installerer. Programmene som sniker seg med kan servere annonser, endre DNS-innstillinger, klikke på annonser i bakgrunnen, laste opp nettleserhistorikk og informasjon om maskinen osv. Noen ganger blir også ren skadevare installert. Det blir stadig vanskeligere å definere hva som er skadevare og ikke.



Gjennomsnittlig antall alvorlige hendelser per kunde per måned

5 HENDELSER OG MØRKETALL

Resten av rapporten er basert på besvarelser fra 412 av de 1500 virksomhetene. Disse har fortalt mer om den alvorligste sikkerhetshendelsen de opplevde i perioden og hvilke konsekvenser den fikk.

Virus og skadevare forårsaker de verste hendelsene for norske virksomheter. Av undersøkelsen kom det fram at 132 virksomheter (32%) ble rammet av uspesifiserte virus eller annen skadevare. Alvorligheten av slik skadevare er variert. For 58 virksomheter (14%) var løsepengevirus den verste hendelsen, og flere av disse mistet filer, mens 40 virksomheter (10%) oppga spam som sin alvorligste sikkerhetshendelse.

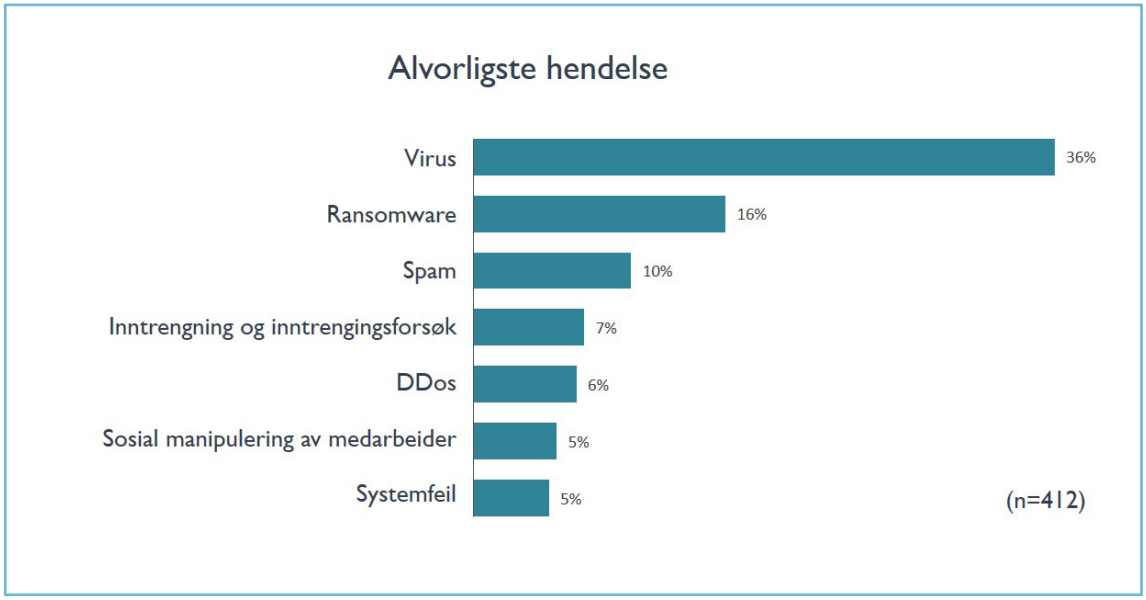
Den mest vidtrekkende konsekvensen er oppgitt å være ekstra arbeid i form av arbeidstimer (41%), og deretter følger tapt eller eksfiltrert data (16%). Kun 12% oppgir at de har hatt direkte kostnader. 53 virksomheter (13%) aner ikke hvilke konsekvenser hendelsen har hatt. Det som derimot er tydelig er at hendelsen har hatt konsekvenser i en eller annen form for mange av virksomhetene som har svart. Egen arbeidsinnsats til hendelseshåndtering utgjør også selvsagt et økonomisk tap. Utsagn som *«Dette påvirket daglig drift, forespørsler som kommer inn kunne ikke bli besvart, og dette kunne få økonomiske konsekvenser», «Alt ble ødelagt og tok enorme ressurser for å lete fram i andre systemer for å sette det tilbake igjen» og «Det alvorligste var at dette var før sommersesongen. Vi fikk ikke sett hvilke kunder som hadde bestilt eller som skulle komme på hotellet. Alt var slettet, og vi kunne heller ikke booke nye gjester siden vi ikke hadde noen oversikt over de som allerede var booket»* illustrerer vanskelighetene enkelte virksomheter opplevde.

Undersøkelsen viser at inntrengning i datasystemene, systemfeil og virus hovedsakelig førte til tapte arbeidstimer. Med ransomware, derimot, er tapte data den klart største konsekvensen, etterfulgt av arbeidstimer. Konsekvensene er mer sammensatte dersom virksomheten blir utsatt for spam og sosial manipulasjon. Her fordeler konsekvensene seg på tap av data, direkte økonomiske konsekvenser, arbeidstimer og ukjente konsekvenser.

Over 50 av virksomhetene aner ikke hvor mye hendelsen kostet dem, og det er en tendens til å undervurdere disse kostnadene. En bedrift som fikk filene på en server kryptert rapporterte at hendelsen ikke kostet dem noe til tross for at det nødvendigvis har gått med noe tid til å gjenopprette filene. En annen bedrift oppga at et løsepengevirus kostet dem 100 kroner, som heller ikke framstår som en realistisk sum. Samtidig oppga enkelte bedrifter betydelige utgifter i forbindelse med den verste sikkerhetshendelsen. For en bedrift med 27 ansatte førte phishing til utgifter på 600 000 kroner, mens en virksomhet innen undervisning med 15 ansatte og delvis outsourcet IT-drift opplevde at partneren ble utsatt for datainnbrudd som førte til at personopplysninger kom på avveie og enorme utgifter.

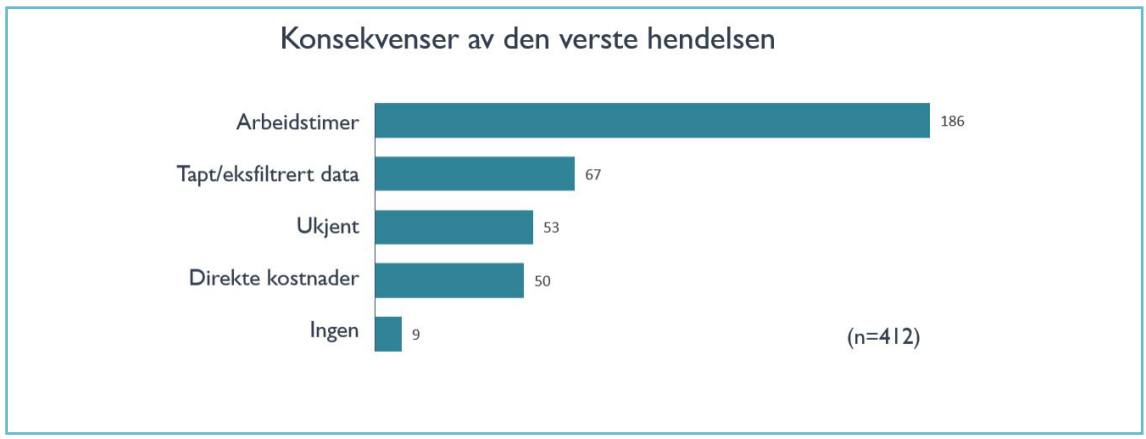
Mangelfulle sikkerhetskopier synes å være et problem for mange mindre selskaper og medfører uunngåelige tap når sikkerhetshendelser inntreffer. En bedrift mistet to måneders regnskap da en maskin sluttet å virke, noe som resulterte i at dette måtte føres inn på nytt, mens en annen virksomhet mistet filer grunnet løsepengevirus og estimerte kostnadene for dette til 1 000 000 kroner. Samtidig førte frykt for spredning av løsepengevirus til dramatiske avgjørelser. En virksomhet «låste ned hele datanettverket», noe som gjorde at 1200 brukere ikke kunne jobbe. En annen tok ned en filserver midlertidig, som fikk konsekvenser i fem kommuner. Undersøkelsen viser at virksomheter som har gode sikkerhetskopier rapporterer om betydelig mindre konsekvenser som følge av løsepengevirusinfeksjoner. Spranget fra noen tapte arbeidstimer til et tap på flere hundre tusen er enormt og viser viktigheten av gode sikkerhetsrutiner.

Det var 21 virksomheter, eller 5%, som oppdaget forsøk på sosial manipulasjon av medarbeidere i løpet av 2015. Konsekvensene av slike angrep kan være alvorlige, fordi medarbeidere kan brukes til å omgå sikkerhetsrutiner eller lures til å dele tilsynelatende harmløs informasjon som kan brukes i senere angrep. I sin trusselvurdering advarer NSM mot direktørsvindler som har rammet flere norske virksomheter i år. I slike angrep utgir svindleren seg for å være en del av ledelsen i en virksomhet og forsøker å lure en økonomiarbeider til å betale en faktura eller overføre penger til en konto, ofte i utlandet. Utførelsesevnen varierer og norske virksomheter må være forberedt på alt fra automatisk oversatte eposter til falske fakturaer sendt fra en leders kompromitterte epostkonto og svindlere med detaljkunnskap om virksomheten som ringer utvalgte økonomiarbeidere. Gjennomtenkte rutiner rundt betalinger av regninger og trening av ansatte kan redusere sannsynligheten for at slike angrep lykkes og sørge for at de oppdages innen kort tid.



Løsepengevirus rammer norske bedrifter

En virksomhet med 8 ansatte og en omsetning på drøyt seks millioner endte opp med estimerte kostnader på 200 000 kroner etter at en epost som inneholdt løsepengevirus førte til at en server ble kryptert. «Alt ble ødelagt og det tok enorme ressurser for å lete fram filene i andre systemer». Det er en betydelig utgift for en enkeltstående sikkerhetshendelse som langt på vei kan unngås ved hjelp av regelmessige sikkerhetskopier.



Lurt til å overføre 500 millioner kroner

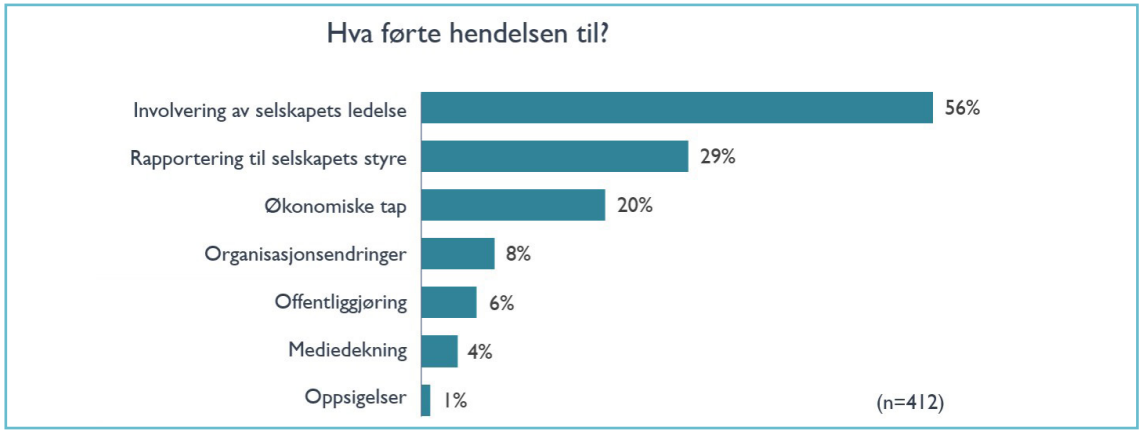
I januar ble det norske datterselskapet i et verdensomspennende konsern oppringt av en mann som utga seg for å være en av konsernets toppledere. Mannen ba datterselskapet overføre millionbeløp til flere kontoer i Asia. Oslo-kontoret overførte i de påfølgende dagene rundt 500 millioner kroner. Derfra beveget pengene seg videre på kryss og tvers over landegrenser.

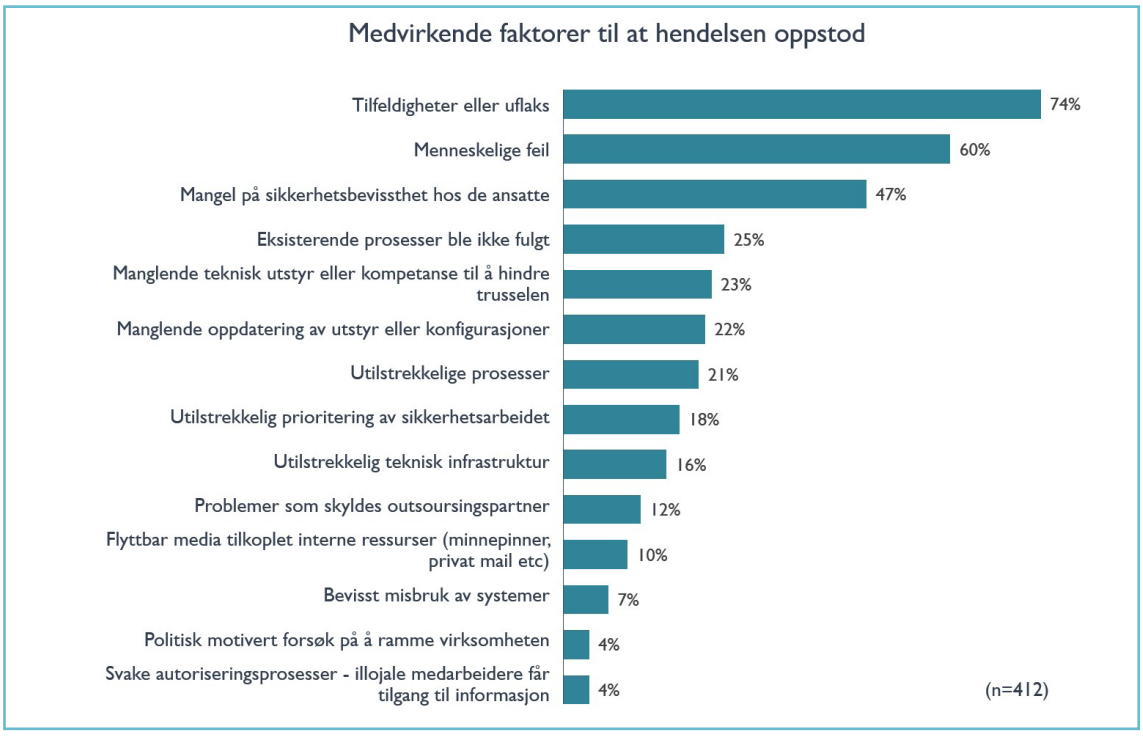
Angrepet ble oppdaget innen kort tid, og politiet klarte derfor å stanse flesteparten av overføringene, men fortsatt er rundt 100 millioner kroner på avveie.

Hva førte hendelsen til?

Kvaliteten på beskrivelsen fra de 412 virksomhetene som svarte på spørsmålet om den verste sikkerhetshendelsen er varierende. Det at de har svart på dette spørsmålet betyr ikke at hendelsen har vært katastrofal. Den kan like gjerne ha medført plunder og heft. Over halvparten av virksomhetene (56%) involverte ledelsen, mens nærmere en tredjedel (29%) valgte å informere styret. Derfor er det noe overraskende at kun 20% av virksomhetene oppgir at hendelsen førte til økonomiske tap. Merk at dette tallet er lavere enn andelen som rapporterer ekstra arbeidsinnsats som følge av hendelsen (41%). Her skjuler det seg økonomiske tap; tid som går med til hendelseshåndtering kan alternativt brukes til andre inntektsgivende oppgaver. Figuren under viser en sammenstilling av hva virksomhetene rapporterte at hendelsen førte til. Bare 6% av hendelsene offentliggjøres, og mørketallene er derfor store.

Virksomhetene oppgir at den verste sikkerhetshendelsen skyldtes tilfeldigheter eller uflaks i 74% av de 412 hendelsene, noe som tyder på at virksomhetene i liten grad oppfatter at angrepene er rettet spesifikt mot dem. Det kommer også fram at medarbeidere i 60% av tilfellene gjorde feil som bidro til at sikkerhetshendelsene oppsto, og i 47% av tilfellene var manglende sikkerhetskompetanse en faktor. Manglende investering i og prioritering av sikkerhetsarbeidet står bak en betydelig andel av hendelsene: utilstrekkelig teknisk infrastruktur (16%), prosesser (21%) og prioritering av sikkerhetsarbeidet (18%), manglende oppdatering av utstyr eller konfigurasjoner (22%), manglende teknisk utstyr eller kompetanse (23%), brudd på prosesser (25%) og manglende sikkerhetsbevissthet hos ansatte (47%).





Løsepengevirus

Klokken er 08:56 da alarmen går i mnemonics døgnbemannede Security Operations Centre (SOC). Det er oppdaget trafikk fra en kunde mot et domene kjent for å spre skadevare. Sikkerhetsanalytikerne analyserer hendelsen og kommer fram til at en av kundens klienter med høy sannsynlighet har blitt infisert av løsepengeviruset TorrentLocker, som hovedsakelig spres ved hjelp av spam og har kryptert filer hos virksomheter verden over siden 2014. Fra slutten av 2015 har det blitt observert flere ondsinnede eposter som utgir seg for å komme fra Posten Norge. Mottakeren fikk beskjed om at en pakke var blitt forsøkt levert, og at de måtte følge en lenke i eposten for å få en hentelapp slik at de kunne hente pakken på nærmeste postkontor. Eposten var skrevet på norsk og brukte Postens logo. Dersom en bruker blir lurt til å trykke på lenken vil de komme til en side som ser ut som Postens ordinære side, hvor de blir bedt om å fylle ut en captcha. Gjør de det, vil de ende opp med å laste ned en fil som bruker standard Adobe PDF-ikon, men som i realiteten er en kjørbar fil som begynner å kryptere filer når offeret forsøker å åpne filen. I dette tilfellet ventet mottakeren en pakke, og eposten framsto derfor som troverdig, så hun trykket seg videre. Trafikken ble ikke hindret av brannmuren, og antivirusprogrammet oppdaget heller ikke at en ondsinnet fil var kommet seg inn på klienten. Løsepengevirus kan også kryptere nettverksområder og har derfor et betydelig skadepotensiale. Når filene først er kryptert er de i de fleste tilfeller tapt, med mindre man har sikkerhetskopi eller betaler løsepengene. Sistnevnte anbefales ikke, fordi man ved å betale er med på å finansiere kriminelle nettverk og motivere nye angrep. Derfor gjelder det å avdekke slike angrep innen kort tid. Kunden ble i dette tilfellet varslet innen få minutter og fikk tatt klienten av nett og reinstallert den før infeksjonen spredde seg. Dessverre har vi også tilfeller hvor kunder mister flere ukers arbeid fordi det ikke finnes sikkerhetskopier av arbeidsfiler på klientene som blir infisert.


posten

Du har uforløste pakken

Pakken **CT478625NO** kom på **12/12/2015**. Courier var ute av stand til å levere denne pakken til deg.

- Få og skriv ut adresselapp og vise det på nærmeste postkontor for å få pakken.

Få en adresselapp

Dersom pakken ikke er mottatt innen 30 virkedager Posten Norge vil ha rett til å kreve erstatning fra deg for det er å holde i mengden av 55 kr - for hver dag å holde. Du kan finne informasjon om fremgangsmåten og vilkårene i pakken holde i nærmeste kontor.

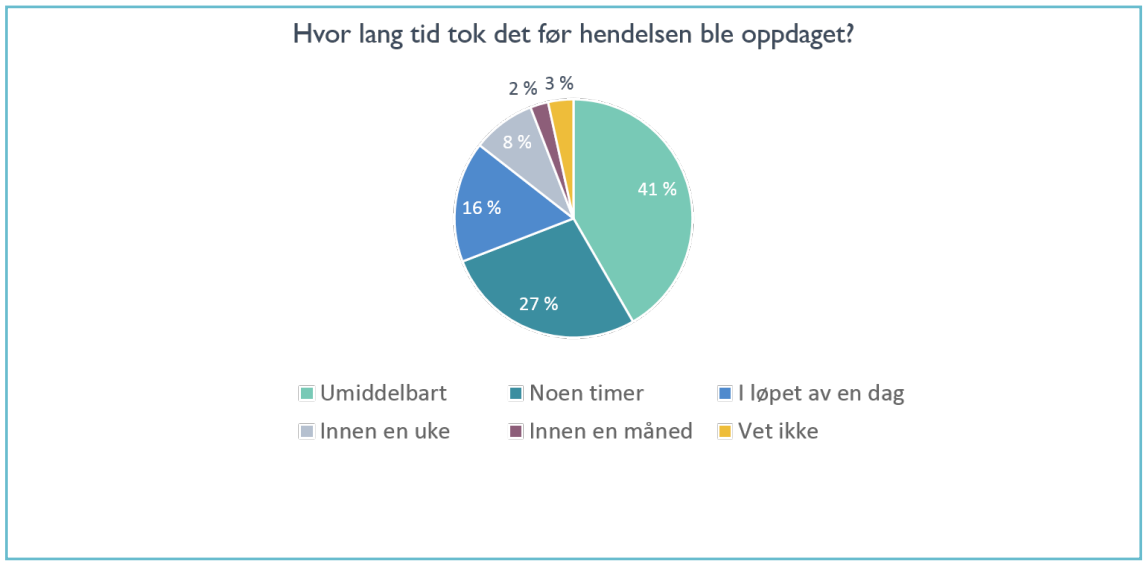
Dette er en automatisk generert melding. Klikk her for å melde deg ut

Hvordan ble så hendelsen oppdaget?

Ifølge svarene oppdaget 46% hendelsen ved en tilfeldighet, 34% ved negativ effekt på drift og 32% ved rutinemessig sikkerhetsmonitorering.

Hvor lang tid tok det før hendelsen ble oppdaget?

Undersøkelsen viser at de fleste hendelsene ble oppdaget i løpet av kort tid. Hele 84 % av hendelsene ble oppdaget i løpet av samme dag. Ingen av de 412 virksomhetene har svart lenger enn 100 dager, men 3% var usikre på når hendelsen inntraff. Ved første øyekast virker det positivt at 90% av hendelsene ble oppdaget i løpet av en uke. Men når 80% av hendelsene oppdages ved tilfeldigheter eller på grunn av den direkte effekten på virksomhetens drift tyder dette på at de fleste virksomheter ikke har nødvendige mekanismer på plass for å oppdage sikkerhetshendelser. Trolig kan mange virksomheter være kompromitterte uten å oppdage dette selv, i tråd med andre internasjonale rapporter og undersøkelser.



Bedriftshemmeligheter på avveie:

Få dager før påskeferien oppdaget en IT-ansatt hos Ulstein Group noe uventet; en Microsoft Exchange Server var i ferd med å fylles av filer for andre gang på kort tid. Den første gangen det skjedde ryddet IT-avdelingen på serveren, men nå begynte trafikken å bli mistenkelig. På serveren oppdaget de at det var lagret krypterte filarkiv med ukjent innhold, og filene var på vei ut av virksomheten. De slo alarm og stengte alle systemer.

Ansatte som planla å arbeide fra hytta fikk beskjed om at det var IT-problemer, konsulenter ble hentet inn og Nasjonal Sikkerhetsmyndighet (NSM) bisto i granskningen av det som skulle vise seg å være en alvorlig sikkerhetshendelse. Den første uken kunne de ikke fortelle de ansatte noe, for det var fortsatt uavklart om angriperen var en utro tjener eller en ekstern trusselaktør.

Før angrepets omfang var kjent kunne de heller ikke bruke noen av virksomhetens potensielt kompromitterte systemer, inkludert epost. De som var involvert i hendelseshåndteringen holdt kontakten på SMS til de følte seg sikre på at inntrengeren var kastet ut av systemet.

Ulstein tror at inntrengeren hadde vært inne på systemet i overkant av en uke og hadde hatt tilgang til flere filservere. NSM klarte å dekryptere en komprimert fil som ikke var blitt sendt ut. Den inneholdt filer relatert til virksomhetens innovasjonsprosjekter. Rundt 500 gigabyte ble stjålet, og bedriftshemmeligheter kan ha kommet på avveie.

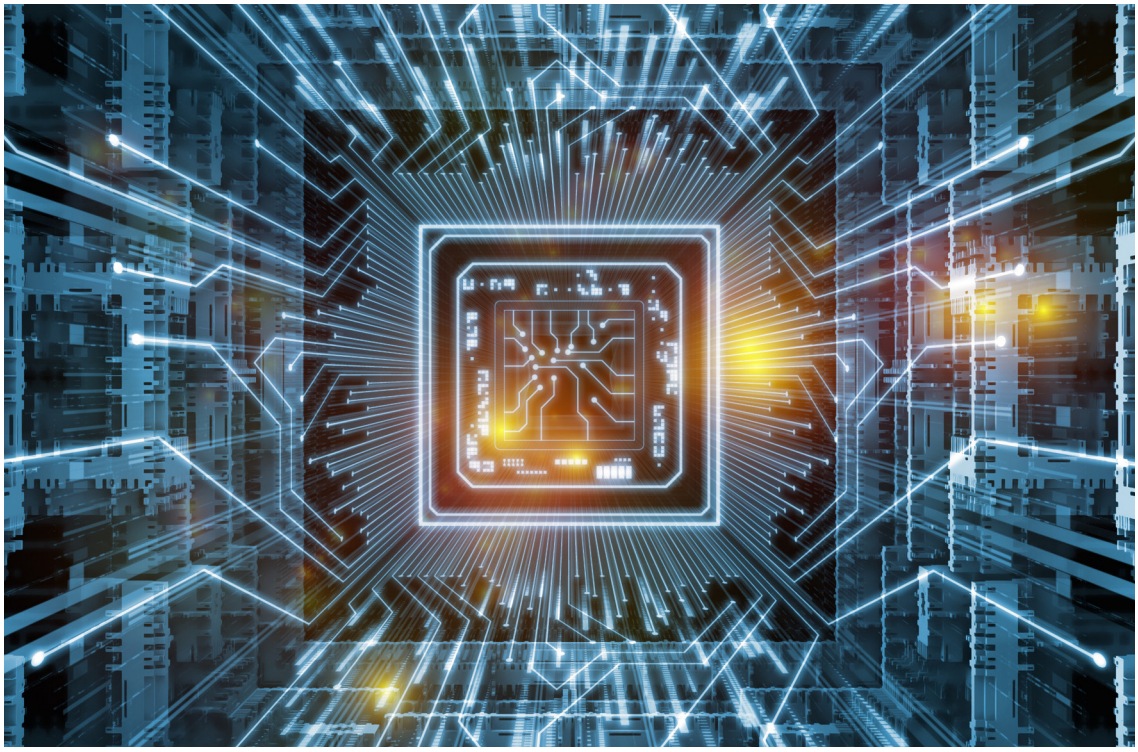
Etterforskningen avdekket kinesiske tegn, og NSM konkluderte med at datakraften som ble brukt og angrepets kompleksitet tydet på at dette var et rettet angrep fra en avansert trusselaktør.

Etter råd fra Politiets Sikkerhetstjeneste (PST), som ble involvert da det oppsto mistanke om angrep fra en annen stat, valgte Ulstein å anmelde hendelsen og kontakte media. Anmeldelsen ble henlagt etter et år, men Ulstein mottok ros for sin åpenhet om angrepet og er glade for at de valgte å stå fram.

For virksomheten var angrepet en vekker og de har i etterkant både tatt flere grep for å gjøre det vanskeligere for angripere å bevege seg rundt i systemet uten å bli oppdaget, slik at et tilsvarende angrep ville kunne oppdages tidligere, og kartlagt sine verdier. Men virksomheten har måttet erkjenne at tekniske løsninger bare er en del av løsningen. Når hver bruker i systemet er en mulig vei inn til virksomhetens verdier, er den menneskelige faktoren sentral.

Noen av de største aktørene i den maritime klynga på Sunnmøre dannet i etterkant av denne hendelsen et IT-sikkerhetsnettverk som jevnlig møtes for å utveksle erfaringer og dele kunnskap.

6 MØRKETALL OG ETTERSPILL



Hvordan ble hendelsen rapportert?

De fleste, 80 %, rapporterte hendelsen til administrator av det aktuelle tekniske systemet. Deretter følger antivirusleverandør med 24%, ISP med 11% og politiet med 9%. Svært få rapporterte til noen av CERTene eller andre myndigheter. At virksomhetene hovedsakelig velger å håndtere hendelsene internt uten å varsle andre kan ha sammenheng med at de fleste virksomhetene i undersøkelsen var små.

Årsaker til at hendelsen ikke ble rapportert

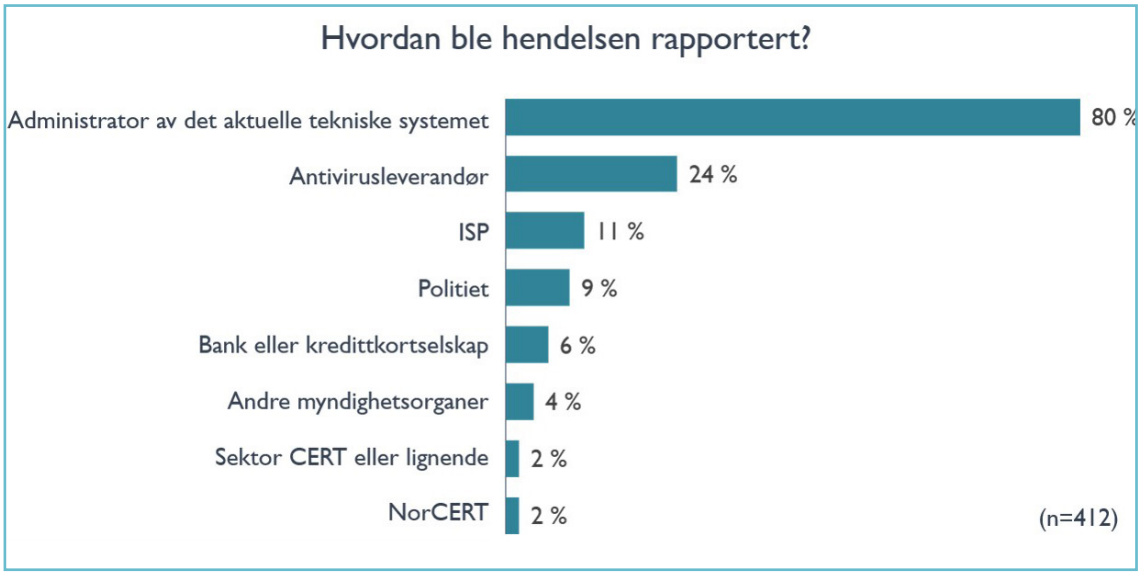
Årets spørreundersøkelse går ikke inn på hvorfor så få anmelder hendelser, men i Mørketallsrundersøkelsen fra 2014 kom det fram at flertallet ikke trodde det ville være mulig å finne gjerningsmannen, mens andre manglet tiltro til politiets kompetanse.

Politiet mottok 51 anmeldelser for datainnbrudd i 2015, men ettersom så få anmelder angrep er det naturlig å anta at det faktiske antallet datainnbrudd er høyere. Det er en utfordring for politiet å spore kriminalitet på nett. En angriper som holder til i Frankrike kan bruke utstyr i Kina til å angripe en norsk virksomhet og samtidig få det til å se ut som angrepet kommer fra Australia. Sakenes kompleksitet fører ofte til henleggelse, men virksomheter som angripes bør likevel vurdere å anmelde. Dersom mørketallene blir mindre får politiet et klarere bilde av dagens situasjon, noe som kan føre til at arbeidet med slik kriminalitet prioriteres høyere og politiets kompetanse øker.

På spørsmålet om hvem som sto bak den mest alvorlige hendelsen var det 22% som svarte, og kun et mindretall av disse visste hvem som sto bak. Svarene spriker fra egne ansatte til elever ved skolen, kunder, russiske servere, Kina, IT-leverandører og kjenninger av politiet. At så få kunne svare på hvem som sto bak kan tyde på at disse hendelsene kun etterforskes av virksomheten i begrenset grad.

Endringer i organisasjonen som resultat av hendelsen

Nesten halvparten av virksomhetene, 44%, gjorde endringer i policy eller rutiner i kjølvannet av den alvorligste hendelsen, mens 25% investerte i sikkerhetsutstyr. Videre var det 20% som utviklet sikkerhetsprosesser og etablerte et sikkerhetsmiljø, og et tilsvarende antall leide inn en tjenesteleverandør til å håndtere sikkerheten. Det var 13% som outsourcet sikkerhetsfunksjonene, mens kun 3% ansatte flere folk med sikkerhetskompetanse. Det lave tallet nye ansatte kan skyldes at det var en hovedvekt av mindre bedrifter i undersøkelsen.



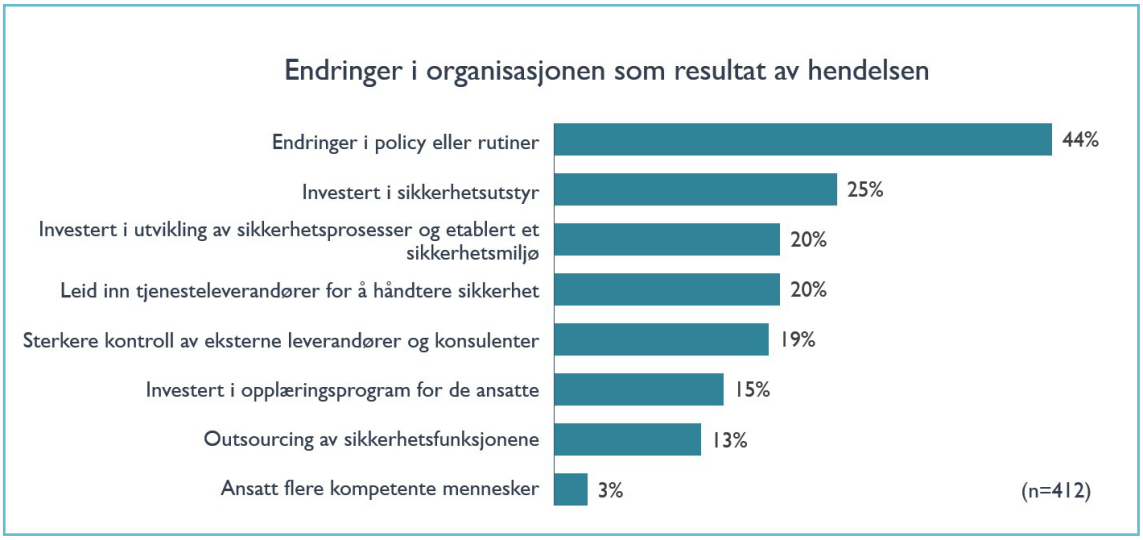
Avviksmeldinger til Datatilsynet

Det er i dag en plikt i Personopplysningsloven om å varsle Datatilsynet dersom konfidensielle personopplysninger har kommet på avveie. I mai 2018 får vi et nytt personvernregelverk (en EU-forordning) som innebærer strengere regler for håndtering av sikkerhetsbrudd.[2] Forordningen stiller krav til når det skal varsles, hva varselet skal inneholde og hvem som skal varsles. Kort sagt skal man si fra raskere og oftere enn man gjør i dag.

2. Les mer om avviksmeldinger og forordningen til Datatilsynet her:

https://www.datatilsynet.no/Sikkerhet-internkontroll/Avviksmeldinger-til-Datatilsynet/

https://www.datatilsynet.no/forordning



7 ANBEFALTE SIKRINGSTILTAK

Sikkerhetskopier

Løsepengevirus er et voksende problem, og flere virksomheter i undersøkelsen fortalte at infeksjon av slike virus førte til tap av data og arbeidstimer. Derfor blir sikkerhetskopier og rutiner for hurtig gjenopprettelse stadig viktigere.

- Innfør jevnlig sikkerhetskopiering av virksomhetens data
- Ha rutiner for gjenopprettelse av data, og test at disse fungerer

Medarbeideres sikkerhetsbevissthet

Medarbeideres feil og manglende kompetanse bidro til at sikkerhetshendelser oppsto i flere hundre av virksomhetene som ble intervjuet i denne undersøkelsen.

- Sørg for at medarbeidere kjenner virksomhetens sikkerhetsrutiner og forstår hvorfor rutinene må følges.
- Øk medarbeideres sikkerhetsbevissthet, eksempelvis ved hjelp av opplæringspakker fra NorSIS og intern trening. Nasjonal sikkerhetsmåned arrangeres hver oktober og kan brukes til å gi medarbeidere innsikt i trusselbildet og hvordan de ved å følge virksomhetens sikkerhetsprosesser kan minske faren for uønskede hendelser.
- Økonomimedarbeidere bør få opplæring om sosial manipulering, og virksomheten bør innføre rutiner rundt overføringer av større beløp som gjør det vanskeligere for direktørsvindlere å lykkes.

Deteksjon

Nærmere 70% av virksomhetene oppdaget sin verste sikkerhetshendelse enten ved en tilfeldighet eller fordi den hadde negative innvirkninger på driften. Norske virksomheter må styrke sin evne til å oppdage og håndtere sikkerhetshendelser. Angrepet mot Ulstein Group viser også viktigheten av å kunne oppdage mistenkelig trafikk innad i systemet.

Styrk evnen til å detektere angrep:

- Ha overvåkningssystemer for oppdagelse av hendelser (Intrusion Detection System)
- Sørg for at antivirussystemer og loggføring er på plass
- Ha rutiner for å følge opp alarmer og logger

Grunnleggende tiltak for mindre virksomheter

Undersøkelsen viser at norske virksomheter fortsatt lider økonomiske tap fra sikkerhetshendelser som kunne vært unngått ved hjelp av grunnleggende tiltak. NSMs fire tiltak mot dataangrep[3] kan stoppe en stor del av angrepene mindre virksomheter utsettes for:

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

Systematisk sikkerhetsarbeid

For mellomstore og store bedrifter er det viktig å sette sikkerhetsarbeidet i system. Styringssystemer for informasjonssikkerhet – som ISO 27001 eller ISO9001 – er nyttige i dette arbeidet. DIFIs veileder for informasjonssikkerhet, som er basert på ISO 27001, er et godt utgangspunkt. Her tilbys gratis maler og andre verktøy som kan benyttes direkte ute i virksomhetern Det finnes også bransjespesifikke styringssystemer, som Normen for Helse- og omsorgssektoren.[4]

3. Les mer på: https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/system-teknisk-sikkerhet/s-01-fire-effektive-tiltak-mot-dataangrep.pdf

4. Se: http://internkontroll.infosikkerhet.difi.no

http://normen.no/

Mørketall

Norske virksomheter må ta et oppgjør med unødvendig hemmelighold og arbeide med å få ned mørketallene. Det å anmelde sikkerhetshendelser til politiet er et langsiktig tiltak; reduserte mørketall gir politiet dokumentasjonen som trengs til å prioritere kompetanseheving og ressurser til å håndtere slik kriminalitet. Tilsvarende kan mediedekning føre til økt kunnskap om truslene norske virksomheter står overfor: det kan gi andre virksomheter tid til å innføre tiltak mot nye angrepsmetoder, som for eksempel direktørsvindel.

- Anmeld hendelsen på det lokale politikontoret
- Vurder å kontakte media

Med støtte fra

POLITIET
POLITIDIREKTORATET

BDO

Finans Norge

mnemonic
- securing your business

telenor

Norges vassdrags- og energidirektorat
NVE

NSM