Rapport

Coronaviruspandemins inverkan på den digitala säkerheten

VAHTI / Rousku Kimmo (DVV)

Hantering av dokument

Ägare	VAHTI-ledningsgruppen
Upprättat av	Kimmo Rousku – kimmo.rousku@dvv.fi
Granskat av	Erja Kinnunen
Godkänt av	VAHTI-ledningsgruppen digiturva@dvv.fi

Versionshantering

version nr	åtgärder	datum/person
0.90	Utkast	KR 9.6.2020
0.95	Uppdaterat utkast	EK 10.6.2020
0.99	VAHTI-ledningsgruppens presentationsversion	KR 10.6.2020
1.00	Version behandlad av VAHTI-ledningsgruppen	11.6.2020 KR

VAHTI / Rousku Kimmo (DVV)

Innehållsförteckning

VAHTI / Rousku Kimmo (DVV)

Rapport

Allmänt

Denna rapport har utarbetats av ledningsgruppen för digital säkerhet inom den offentliga förvaltningen (VAHTI), som verkar vid Myndigheten för digitalisering och befolkningsdata (MDB). För att producera rapportens innehåll ordnade VAHTI-sekretariatet en enkät om koronaviruspandemin, som gav 136 svar. Resultaten har indelats i fyra kategorier enligt respondenternas verksamhetsområde.

Detta är rapportens version 1.0. Vi kompletterar rapportens branschspecifika resultat under sommaren och publicerar version 2.0 i augusti.

Syftet med rapporten är bland annat att

- utreda hur organisationerna inom den offentliga förvaltningen har lyckats med den digitala verksamhetsförändringen under coronaviruspandemin våren 2020, till exempel med att ordna distansarbete och producera digitala tjänster
- beskriva vilka hot mot verksamheten och tjänsterna organisationerna har identifierat samt hur hoten och riskerna som de orsakat har behärskats
- identifiera hurdan hjälp och vilket stöd organisationerna inom den offentliga förvaltningen önskar av VAHTI

Rapporten skickas för kännedom till organisationer inom den offentliga förvaltningen samt till alla medlemmar i VAHTI-ledningsgruppen och VAHTI-expertgruppen. Vi presenterar rapporten för de centrala intressentgrupperna och informerar om resultaten och om nödvändiga åtgärder för att utveckla den digitala säkerheten vid evenemangen hösten 2020.

Rapportens målgrupper är organisationens ledning samt ansvarspersoner och experter som ansvarar för den digitala säkerheten (riskhantering, verksamhetens kontinuitet och beredskap, datasäkerhet, cybersäkerhet samt dataskydd).

MDB ansvarar för att samla in en helhetsbild av den offentliga förvaltningens digitala säkerhets olika delområden. I det pågående projektet för utveckling av den digitala säkerheten inom den offentliga förvaltningen (JUDO) genomförs en digital tjänst, med hjälp av vilken vi under de kommande åren kan genomföra motsvarande enkäter. Syftet med tjänsten är att samla aktuell information om digital säkerhet samt att för organisationer inom den offentliga förvaltningen producera rapporter om det egna läget i fråga om digital säkerhet och jämförelseuppgifter om andra motsvarande organisationer.

VAHTI / Rousku Kimmo (DVV)

Ledningens sammandrag

Påskyndat digitalt kliv

I mars 2020 orsakade den globala pandemin orsakad av coronaviruset och den därav föranledda övergången till lagstiftning om undantagsförhållanden en helt ny situation för organisationer inom den offentliga förvaltningen. Majoriteten av personalen hänvisades till distansarbete i huvudsak hemifrån, men samtidigt måste man säkerställa att myndigheternas lagstadgade eller i övrigt kritiska uppgifter och tjänster produceras i en snabbt förändrad situation. Organisationerna måste producera e-tjänster avsedda för medborgarna både i den fysiska och digitala miljön och säkerställa att de nödvändiga tjänsternas prestanda skalades.

Enligt en förhandsbedömning ansågs det vara mycket svårt att lyckas med en sådan förändring. På basis av denna och andra enkäter kan man dock i efterhand bedöma att förändringen genomfördes väl, delvis till och med mycket bra. Även i andra stater har man genomfört ett motsvarande "digitalt kliv", men till exempel enligt Eurofounds[1] undersökning övergick nästan 60 procent av personalen i Finland till distansarbete, vilket är mer än i något av de 26 länder som deltog i jämförelsen. En av de organisationer som svarade konstaterade att 92 procent av deras personal övergick till distansarbete mycket snabbt och framgångsrikt.

Goda resultat av långsiktig digitalisering

Framgången som beskrivs ovan är inte bara en slump eller lycka, utan resultatet av utvecklingen av ett långsiktigt, systematiskt digitalt samhälle. Detta syns bland annat i att Finland förblev nummer ett i DESI-indexet 2020[2] I Finland har man länge satsat betydligt på digitalisering av verksamheten, elektroniska tjänster samt tjänster som riktar sig till personal och medborgare. Finland har länge varit den nation som använder mest mobildataförbindelser i världen[3] och de processer och den tekniska utrustning som distansarbetet förutsätter har varit väl tillgängliga. En observation i enkäten var att det i vissa områden har förekommit tillfälliga problem med tillgången till vissa ICT-apparater (till exempel bärbara datorer, skärmar och hörlurar med mikrofon), men på grund av fungerande logistikkedjor har dessa inte skapat ett större problem.

Coronatiden ökade antalet hot, men man har kunnat reagera på dem

Coronaviruspandemin har krävt alla fem delområden inom digital säkerhet utvecklas. I enkäten framfördes 12 allmänna hot. Även om vart och ett av dem hade förverkligats i minst en av de organisationer som svarade på enkäten, hade man lyckats hantera dessa hot och de risker som de medfört bra.

I svaren framkom tre hot som hade förekommit hos minst hälften av respondenterna:

[1] https://www.eurofound.europa.eu/sites/default/files/ef_publication/field_ef_document/ef20058en.pdf
[2] https://ec.europa.eu/digital-single-market/en/desi
[3] https://www.traficom.fi/sites/default/files/media/file/Telecommunications-Markets-in-the-Nordic-and-Baltic-Countries-2018.pdf

Störningar i anslutning till distansarbetsförbindelserna 81%
Störningar i datakommunikationskapaciteten 62%
Nya slag av bedrägeri- eller attackmeddelanden via e-post 59 %

Även om mängden datakommunikation nationellt och internationellt har ökat betydligt har operatörerna kunnat garantera den prestationsförmåga och överföringskapacitet som behövs i Finland. I en del av tjänsterna har det förekommit fördröjningar och funktionella avbrott på grund av betydligt ökade användarmängder, detta syns som ovan nämnda störningar i distansarbetsförbindelserna (81 procent) och datakommunikationskapaciteten (62 procent). Samma fenomen har iakttagits också när tjänster utanför Finland används. De flesta av oss har lagt märke till att nätbrottslingarna på ett smidigt sätt har ändrat sina bedrägerimetoder för att utnyttja Covid-19/ och coronaviruspandemiteman, vilket syns som nya bedrägeri- eller anfallsmeddelanden (59 procent).

Den funktionella förändringen har krävt många förändringar såväl i produktionen av ICT-tjänster som i personalens arbetssätt. Eftersom förändringarna gjordes på mycket kort tid har till exempel grundliga konsekvensbedömningar, hotbedömningar och riskbedömningar med anknytning till förändringarna inte varit möjliga. I många organisationer kan en del av personalen ha distansarbetat för första gången, varvid tillämpningen och utvecklingen av befintliga anvisningar och processer samt personalens snabbanvisningar och utbildning har haft en central roll.

Delområden som kräver särskild uppmärksamhet

Tills vidare har det i Finland inte skett omfattande eller annars betydande dataintrång, dataläckage eller cyberattacker som kunnat kopplas samman med pandemin. Detta innebär inte att organisationerna inte bör fortsätta att utveckla den digitala säkerheten. Av tolv hot mot den digitala säkerheten visar tre av de minst förverkligade att man även i fråga om tjänsternas tillgänglighet och integritet, uppgifternas konfidentialitet och dataskydd måste fortsätta att aktivt utveckla tjänsterna.

Överbelastningsattacker 10%
8% Läckage av sekretessbelagd information
Förlust av data och program 1%

Av dessa är i synnerhet överbelastningsattacker och läckage av sekretessbelagda uppgifter hot som om de genomförs kan orsaka betydande problem i organisationens verksamhet. När det gäller kritiska tjänster kan de till och med skada hela samhället, vilket kan leda till att medborgarnas förtroende förloras.

Vilken hjälp önskar respondenterna få?

I enkäten bad vi respondenterna framföra önskemål om hurdan hjälp de skulle vilja ha i fortsättningen eller hur den exceptionella situationen våren 2020 i övrigt borde beaktas i utvecklingen av verksamheten. Mest önskade man enhetliga anvisningar för tryggandet av säkerheten hos de kommunikationstjänster som används gemensamt samt för distansarbetet. En annan sak som togs upp var behovet av att samordna och förenhetliga myndigheternas enkäter, både vad gäller innehållet och de

tjänster som används. Det tredje önskemålet var att vi tillsammans kunde utveckla saker och ting genom att utnyttja de bästa erfarenheter som samlats in från olika håll och även lära oss av misstag.

Fem centrala observationer

Nedan listas fem centrala observationer som framgick av resultaten. Två positiva observationer gäller hur verksamhetsförändringen lyckades och tre gäller utvecklingen av den digitala säkerheten. I varje punkt finns dessutom urval av öppen respons.

1. **Övergången till distansarbete och tekniska lösningar i anslutning till detta har lyckats åtminstone bra, delvis till och med mycket bra, och inga betydande avvikelser har hittills observerats.**

   Ansvarspersonerna och experterna på digital säkerhet ser förändringen i verksamheten under våren som en positiv, mycket lyckad helhet.

   > "Funktions- och serviceförmågan har varit nästan normal sedan början av mars."
   >
   > "Flera funktioner använde redan tidigare distansarbete, även om det inte är i den omfattning som coronasituationen kräver. De mest kritiska funktionerna har dock fortfarande genomförts på verksamhetsställena. "
   >
   > "De största utmaningarna är att nya tjänster och processer har tagits i bruk utan att deras säkerhet har kunnat säkerställas på samma sätt som under normala förhållanden."
   >
   > "För en del av övergången mer utmanande på grund av arbetsuppgifternas karaktär och störningar i distansförbindelserna."

   I april-maj 2020 genomförde Myndigheten för digitalisering och befolkningsdata också fem olika webbsändningar riktade till experter på digital säkerhet. Deltagarna tillfrågades "Hur har arbetet under undantagsförhållandena fungerat?". De 462 respondenternas åsikt stöder resultatet av denna enkät:

   Dåligt 0%
   Nöjaktigt 5%
   Mycket 62%
   Utmärkt 33%

   Övergången till distansarbete har upplevts som en framgång som i fortsättningen säkert kommer att förändra vårt sätt att arbeta, så särskild uppmärksamhet bör fästas vid förändringen. Organisationerna ska säkerställa personalens psykiska välbefinnande[4] och resiliens (krisbeständighet), även när de återvänder till arbetsplatsen.

[4] https://www.ttl.fi/ohje-etatyosta-ja-henkisesta-hyvinvoinnista-tyopaikoille-koronavirusepidemian-ehkaisyyn/

Enligt undersökningar är 95 procent av data- och cybersäkerhetsincidenterna och kränkningarna av personuppgifternas informationssäkerhet en följd av mänsklig verksamhet[5]; misstag som skett vid brådska eller oavsiktligt på grund av den mänskliga faktorn. Utöver oavsiktlig verksamhet ska uppmärksamhet fästas vid verksamhet som strider mot anvisningarna och tekniska lösningar bör utvecklas för att hantera de risker som avsiktlig verksamhet medför. Att utveckla personalens kompetens och motivation är ett av de mest kostnadseffektiva sätten att förbättra organisationens digitala säkerhet.

2. **Tillgången till och säkerheten för lagstadgade tjänster som används eller produceras av organisationerna har hållits på en hög nivå.**

   Även om det av flera svar framgår att mängden e-tjänster till och med har ökat betydligt har inga större problem observerats i de tjänster som riktar sig till medborgare eller kunder. Eventuella problem gäller mer interna lösningar inom organisationen, till exempel tekniska lösningar med anknytning till distansarbete.

   > "Pandemin har inte påverkat de använda datasystemens funktion. Antalet infektioner i Finland är så litet att underhållet av datasystemen inte har störts. ”
   >
   > "Datasystemen och den övriga tekniska miljön har varit stabila under undantagstillståndet och bibehållit sin prestationsförmåga.”
   >
   > "I fråga om dessa krävde övergången till undantagsförhållanden och distansarbete ett betydande extra arbete under några veckor, men tack vare det har systemen erbjudit ett bra stöd för verksamheten.”

3. **Det saknas enhetliga anvisningar och riktlinjer för granskning och säker användning av nya kommunikationssystem och eventuella molntjänster.**

   Av svaren framgår tydligt att en del organisationer har varit tvungna att ta i bruk nya tjänster med mycket snabb tidtabell. Man kan se att det finns mycket varierande tolkningar av användningen av tjänsterna inom olika organisationer inom den offentliga förvaltningen. En del organisationer kan helt ha förbjudit användningen av någon tjänst, andra gör det möjligt att använda tjänsten med hjälp av någon tilläggskontroll och resten av organisationerna tillåter att tjänsten används som sådan.

   > ”Koordinerad analys av riskscenarier, utveckling av beredskap och anvisningar t.ex. i distansarbete (datasäkerhet, dataskydd). Opartisk informationssäkerhetsauditering el. dyl. utvärdering av olika kommunikations- och distansmötesredskap (Meet, Skype, Teams, Zoom) på riksnivå. ”
   >
   > "Det behövs enhetliga och tydliga anvisningar för t.ex. distansarbete i omfattande utsträckning i kommunens funktioner samt för att genomföra de elektroniska funktioner som lagen förutsätter (t.ex. elektronisk signatur)

[5] https://www.researchgate.net/publication/329806166_Botching_Human_Factors_in_Cybersecurity_in_Business_Organizations

genom distansförbindelser. Anvisningar för konfidentialitet inom den elektroniska kundservicen (bl.a. undervisningsväsendet, småbarnspedagogiken), genomförande av den elektroniska kundservicen i praktiken. ”

I Myndigheten för digitalisering och befolkningsdatas webbsändningar frågades "Vilken riktning anser de att den digitala säkerheten har utvecklats under de senaste månaderna?". De 454 svaren fördelade sig på följande sätt:

Förbättrats något 10%
Förblivit oförändrade 47%
Oroväckande riktning 42%
Mycket oroväckande riktning 2%

44 procent av deltagarna i enkäten konstaterade att säkerheten håller på att utvecklas i en oroväckande riktning. På motsvarande sätt har 10 procent av respondenterna upplevt att den digitala säkerheten har förbättrats. Detta beror sannolikt på att organisationerna i fråga har varit tvungna att fästa större uppmärksamhet vid och kanske förbättra datasäkerheten eller beredskapen för störningssituationer. Även om experterna har varit oroliga för säkerhetssituationen, visar vår enkät att dessa problem hittills inte har konkretiserats i någon större utsträckning.

4. Enhetliga anvisningar för distansarbete saknas

Ett tydligt utvecklingsobjekt har att göra med personalens distansarbete och i synnerhet med att säkerställa konfidentialiteten för sekretessbelagda personuppgifter eller personuppgifter som behandlas. En del experter oroar sig för hur sekretessbelagda uppgifter eller personuppgifter hanteras på ett säkert sätt i distansarbete. Dessutom är det oroväckande att när merparten av arbetet utförs på distans blir det betydligt svårare att garantera och övervaka säkerheten än i företagets lokaler.

"Nationell handledning bl.a. vid val av distansarbetsredskap. Riskhanteringsprocesser - hjälp med att välja gemensamma verksamhetssätt. ”

"I distansarbete ökar dataskyddsrisken. Det är rentav omöjligt att övervaka att anvisningarna följs. För en del chefer övervakning av distansarbete främmande. ”

"Jag anser att datasäkerheten och dataskyddet har försämrats en enhet av att den anställde har större ansvar för att sköta ärenden hemma.”

5. Utveckling av en enhetlig lägesbild och processer för insamling av uppgifter om den

Att samla in en "lägesbild" både inom organisationen och mellan myndigheterna nämndes också som ett utvecklingsobjekt med anknytning till säkerheten. Respondenterna har fått många, delvis överlappande förfrågningar från olika myndigheter. Informationssäkerhetsnivån för genomförda enkäter och de rapporteringstjänster som används verkar variera. Enkäten som gjordes för att producera denna rapport genomfördes som en Excel-fil, som de som svarade på enkäten

klassificerade enligt sina egna anvisningar. Svaren skickades i huvudsak in som skyddad e-post.

> "Det fanns inte de uppgifter som behövdes för att skapa lägesbilden, systemen har utvecklats enligt en snabb tidtabell”
>
> "Ett elektroniskt analys- och lägesbildssystem saknas. Word, PowerPoint och e-post betonas för mycket.”
>
> "Vi vet inte alltid hurdan information vi vågar ange som svar på en enkät som skickats till oss, eftersom verktyget inte berättar om dess säkerhet”

VAHTI-ledningsgruppen har behandlat denna rapport vid sitt möte 11.6.2020, och granskade de viktigaste observationerna. Planeringen av nödvändiga utvecklingsåtgärder ges sommaren 2020 till fem VAHTI-arbetsgrupper. Grupperna rapporterar regelbundet om sin verksamhet till ledningsgruppen och presenterar resultaten av sin verksamhet vid VAHTI-evenemangen.

VAHTI / Rousku Kimmo (DVV)

1 Rapportens respondenter och verksamhetsområden

Enkäten om coronaviruspandemin skickades den 11 maj till cirka 490 registratorskontoren inom den offentliga förvaltningens organisation. Svarstiden för enkäten upphörde den 29 maj. Vi vet att flera andra rapporter har begärts av organisationerna under våren och att de har deltagit i många andra enkäter. Att vi fick 136 svar med en svarsprocent på 26 procent kan anses vara bra med tanke på den tillgängliga svarstiden och tidpunkten. Vår erfarenhet visar att det här svarsantalet och -procenten ger en tillräckligt tillförlitlig grund för att skapa en helhetsbild.

Svaren fördelades per verksamhetsområde enligt följande:

1. Kommuner och samkommuner 60 st. 44%
2. Sjukvårdsdistrikt eller annan aktör inom social- och hälsovården 12 st. 9%
3. Statsförvaltningen och den indirekta statsförvaltningen 55 st. 40%
4. Universitet eller annan läroanstalt 9 st. 7%

2 Hur enkäten genomfördes och dess resultat

Enkäten bestod av fem flervalsfrågor och två öppna frågor. De frågade hurdan hjälp organisationerna önskar och bad om respons på enkäten. Man ville hålla enkäten koncist och snabb att besvara eftersom organisationerna samtidigt har varit tvungna att besvara många andra enkäter. Även arbetssituationen för de personer som svarade på enkäten är brådskande på grund av den rådande situationen.

2.1 Frågor

2.1.1 Hur de lagstadgade uppgifterna förlöper

Den första frågan var "Hur bedömer ni att organisationens lagstadgade uppgifter i genomsnitt har fungerat sedan början av mars 2020?” Syftet med frågan var att utreda hur skötseln av organisationernas lagstadgade uppgifter har fungerat sedan mars 2020. I frågan ville man koncentrera sig på verksamhet som är kritisk för organisationens verksamhet, eftersom det är klart att man i en del organisationer har varit tvungen att prioritera den övriga verksamheten, processerna och tjänsterna.

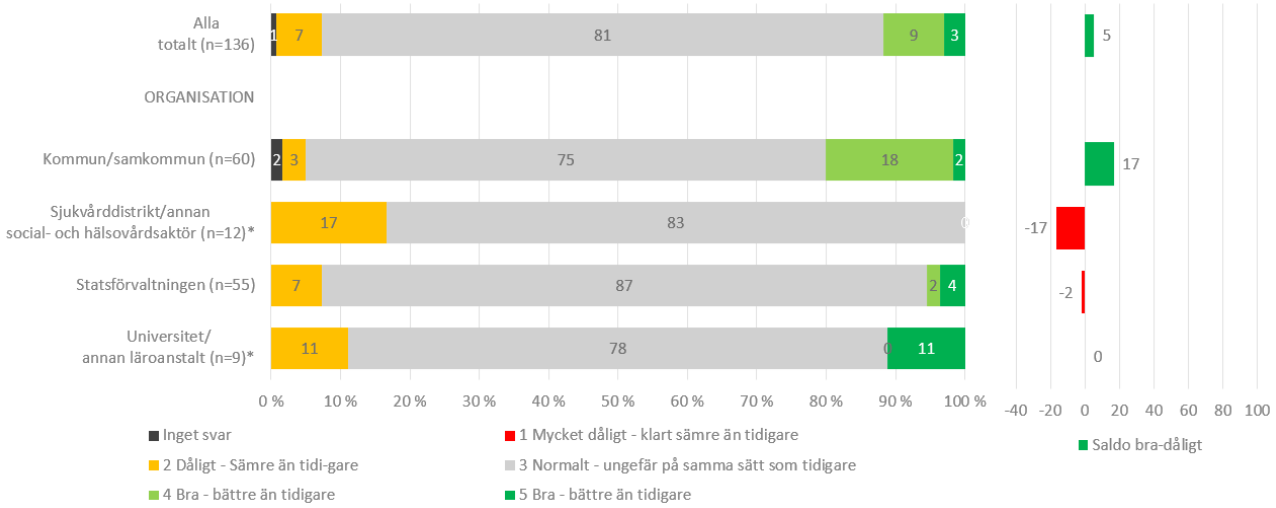

Bild 1. Diagram. Skötseln av de lagstadgade uppgifterna våren 2020.

Som helhet har organisationernas verksamhet i huvudsak genomförts normalt, ungefär på samma sätt som tidigare. De största skillnaderna syns mellan två verksamhetsområden; kommunerna och samkommunerna har kunnat agera betydligt bättre än tidigare och på motsvarande sätt har verksamheten hos sjukvårdsdistrikten och andra aktörer inom social- och hälsovården varit något sämre än tidigare. I genomsnitt är situationen något bättre än tidigare, men skillnaden är inte betydande. Sjukvårdsdistriktens och de övriga social- och hälsovårdsaktörernas situation påverkas sannolikt av den arbetsbelastning som orsakas av coronaviruspandemin samt av administrativa och tekniska förändringar och andra hot mot organisationernas verksamhet.

	Alla totalt	**Kommun/samkommun**	**Sjukvårdsdistrikt/annan social- och hälsovårdsaktör**	**Statsförvaltningen**	**Universitet/annan läroanstalt**
Inget svar	1 %	2 %	0 %	0 %	0 %
1 Mycket dåligt - klart sämre än tidigare	0 %	0 %	0 %	0 %	0 %
2 Dåligt - Sämre än tidigare	7 %	3 %	17 %	7 %	11 %
3 Normalt - ungefär på samma sätt som tidigare	81 %	75 %	83 %	87 %	78 %
4 Bra - bättre än tidigare	9 %	18 %	0 %	2 %	0 %

5 Mycket bra - klart bättre än tidigare	3 %	2 %	0 %	4 %	11 %
Sammanlagt	100 %	100 %	100 %	100 %	100 %

Bild 1. Texttabell. Skötseln av de lagstadgade uppgifterna våren 2020.

2.1.2 Övergång till distansarbete

Kanske var den mest centrala förändringen under coronaviruspandemin behovet av att snabbt och i hög grad övergå till distansarbete. Med frågan "Hur väl har övergången till distansarbete lyckats i er organisation?" ville man utreda om den allmänna positiva bilden av hur saker och ting fungerar i distansarbetet stämmer.

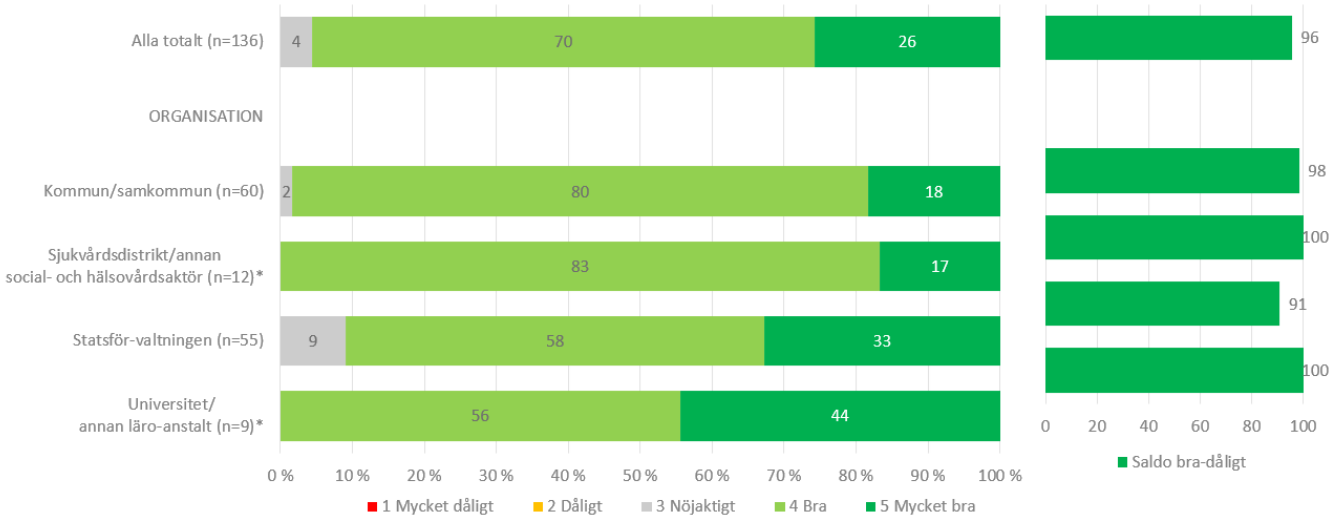

Bild 2. Diagram. Övergång till distansarbete våren 2020.

Svaren visar att distansarbetet har gått bra och rentav mycket bra hos en del respondenter. Ingen uppgav att verksamheten hade försämrats i fråga om distansarbete. Varje bransch är i betydande grad nöjd med verksamhetsförändringen i anslutning till distansarbete. Endast inom statsförvaltningen har 9 procent av respondenterna konstaterat att övergången har skett nöjaktigt.

	Alla totalt	**Kommun/samkommun**	**Sjukvårdsdistrikt/annan social- och hälsovårdsaktör**	**Statsförvaltningen**	**Universitet/annan läroanstalt**
1 Mycket dåligt	0 %	0 %	0 %	0 %	0 %
2 Dåligt	0 %	0 %	0 %	0 %	0 %
3 Nöjaktigt	4 %	2 %	0 %	9 %	0 %

4 Bra	70 %	80 %	83 %	58 %	56 %
5 Mycket bra	26 %	18 %	17 %	33 %	44 %
Sammanlagt	100 %	100 %	100 %	100 %	100 %

Bild 2. Texttabell. Övergång till distansarbete våren 2020.

2.1.3 Stöd för datasystem och tjänster under undantagsförhållandena

Den tredje frågan var "Hur väl har datasystemen och de elektroniska tjänsterna stött verksamheten enligt beredskapslagen?" Med frågan ville man utreda hur övergången till en verksamhet enligt beredskapslagen för första gången i Finlands historia har skett i fråga om datasystem och elektroniska tjänster.

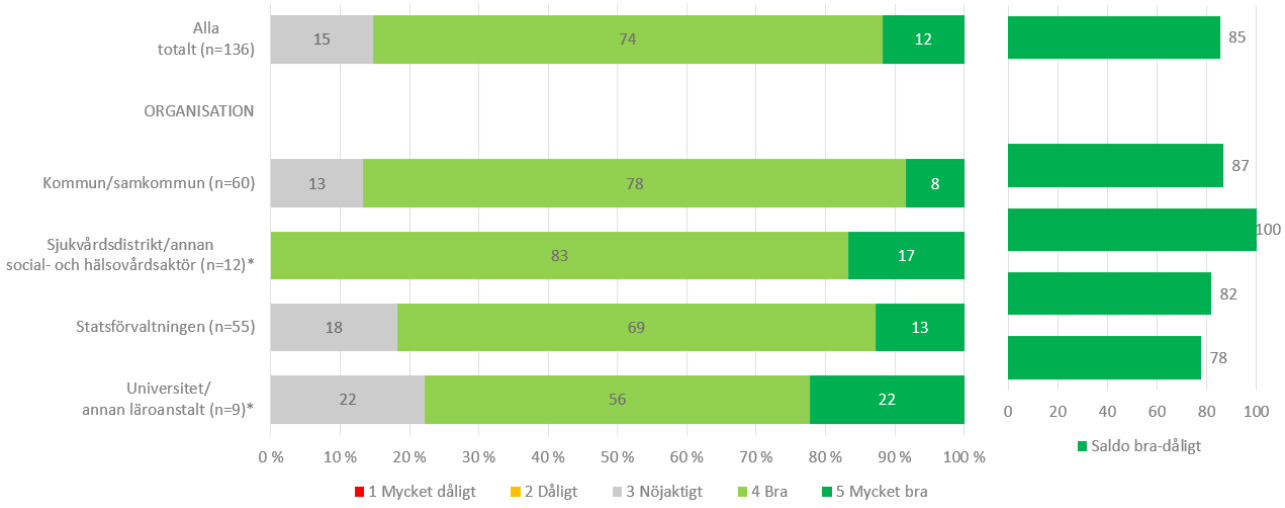

Bild 3. Diagram. Datasystemens och tjänsternas stöd för verksamhet enligt beredskapslagen.

En av de överraskande positiva överraskningarna i enkäten var att enligt svaren har ibruktagandet av beredskapslagen, som tidigare endast gjorts vid olika övningar, i Finland i genomsnitt fungerat bra. Hos en del respondenter till och med mycket bra.

I synnerhet befinner sig sjukvårdsdistrikten och andra aktörer inom social- och hälsovården i en något bättre situation än övriga verksamhetsområden som endast observerar små skillnader.

	Alla totalt	Kommun/samkommun	Sjukvårdsdistrikt/annan social- och hälsovårdsaktör	Statsförvaltningen	Universitet/annan läroanstalt
1 Mycket dåligt	0 %	0 %	0 %	0 %	0 %
2 Dåligt	0 %	0 %	0 %	0 %	0 %
3 Nöjaktigt	15 %	13 %	0 %	18 %	22 %
4 Bra	74 %	78 %	83 %	69 %	56 %
5 Mycket bra	12 %	8 %	17 %	13 %	22 %
Sammanlagt	100 %	100 %	100 %	100 %	100 %

Bild 3. Texttabell. Datasystemens och tjänsternas stöd för verksamhet enligt beredskapslagen.

2.1.4 Genomförandet av digital säkerhet

Den fjärde frågan var "Hur väl har ni kunnat sköta de OLIKA delområdena för digital säkerhet efter början av mars 2020?". Syftet var att utreda hur organisationerna bedömer utvecklingen av verksamheten under coronaviruspandemin inom fem olika delområden enligt referensramen för digital säkerhet. Referensramen för digital säkerhet består av följande delområden:

- Riskhantering
- Verksamhetens kontinuitet och beredskap
- Informationssäkerhet
- Cybersäkerhet
- Dataskydd

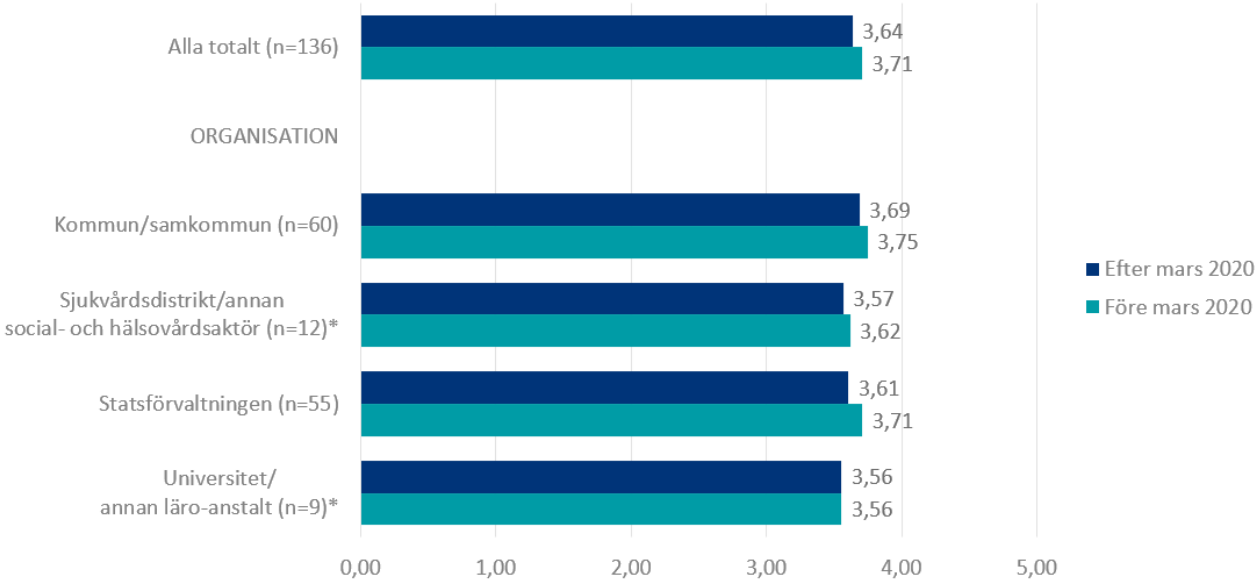

Bild 4. Diagram. Utvecklingen av den digitala säkerheten under våren 2020.

Förhandsförväntningarna angående frågan var att organisationerna skulle berätta att enskilda delområden inom digital säkerhet, såsom informationssäkerhet eller dataskydd, försvagats tydligt till följd av vårens verksamhetsförändring. På basis av svaren kan man konstatera att organisationerna bedömer att de har kunnat sköta den digitala säkerheten nästan lika bra som före coronatiden.

Det medelvärde som uppnåddes före mars är 3,71 (på skalan god-). En försvagning av 0,07 enheter orsakad av coronaviruspandemin kan anses vara liten. Procentuellt sett upplever 37 procent av respondenterna att deras digitala säkerhet har försämrats, men på motsvarande sätt upplever 16 procent att situationen har förbättrats. Som helhet kan bedömningen och bevarandet av den befintliga nivån ses som ett mycket bra resultat.

	Alla totalt	**Kommun/samkommun**	**Sjukvårdsdistrikt/annan social- och hälsovårdsaktör**	**Statsförvaltningen**	**Universitet/ annan läro-anstalt**	**Genomsnitt**
Hur väl har ni kunnat sköta de OLIKA delområdena för digital säkerhet efter början av mars 2020?	3,64	3,69	3,57	3,61	3,56	3,61
Före mars 2020	3,71	3,75	3,62	3,71	3,56	3,67
Skillnad	-0,07	-0,06	-0,05	-0,10	0,00	-0,06

Bild 4. Texttabell. Utvecklingen av den digitala säkerheten under våren 2020.

Från föregående diagram kan man skapa en annan bild som bättre beskriver utvecklingen av digital säkerhet per verksamhetsområde. Situationen har försämrats mest procentuellt, men å andra sidan även förbättrats, i kommunerna och samkommunerna. I denna grupp ansåg 43 procent av respondenterna att den digitala säkerheten har försämrats och 18 procent ansåg att den har förbättrats.

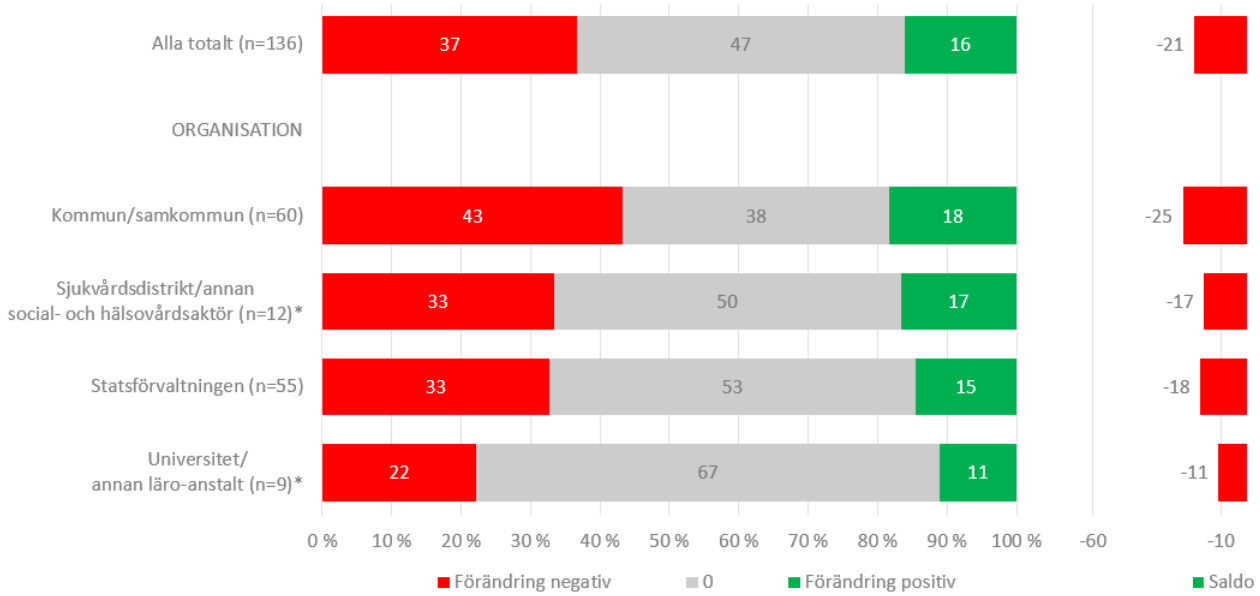

Bild 5. Diagram. Utvecklingen av den digitala säkerheten per verksamhetsområde under våren 2020.

	Alla totalt	**Kommun/samkommun**	**Sjukvårdsdistrikt/annan social- och hälsovårdsaktör**	**Statsförvaltningen**	**Universitet/annan läroanstalt**
Försämrats	37 %	43 %	33 %	33 %	22 %
Bevarats på samma nivå	47 %	38 %	50 %	53 %	67 %
Förbättrats	16 %	18 %	17 %	15 %	11 %
Sammanlagt	100 %	100 %	100 %	100 %	100 %

Bild 5. Texttabell. Utvecklingen av den digitala säkerheten per verksamhetsområde under våren 2020.

2.1.5 Svarens medeltal

I detta stycke har vi beräknat medeltalet för de fyra föregående frågorna, som gör det möjligt att bedöma skillnaderna mellan olika verksamhetsområden - eller snarare avsaknaden av dem.

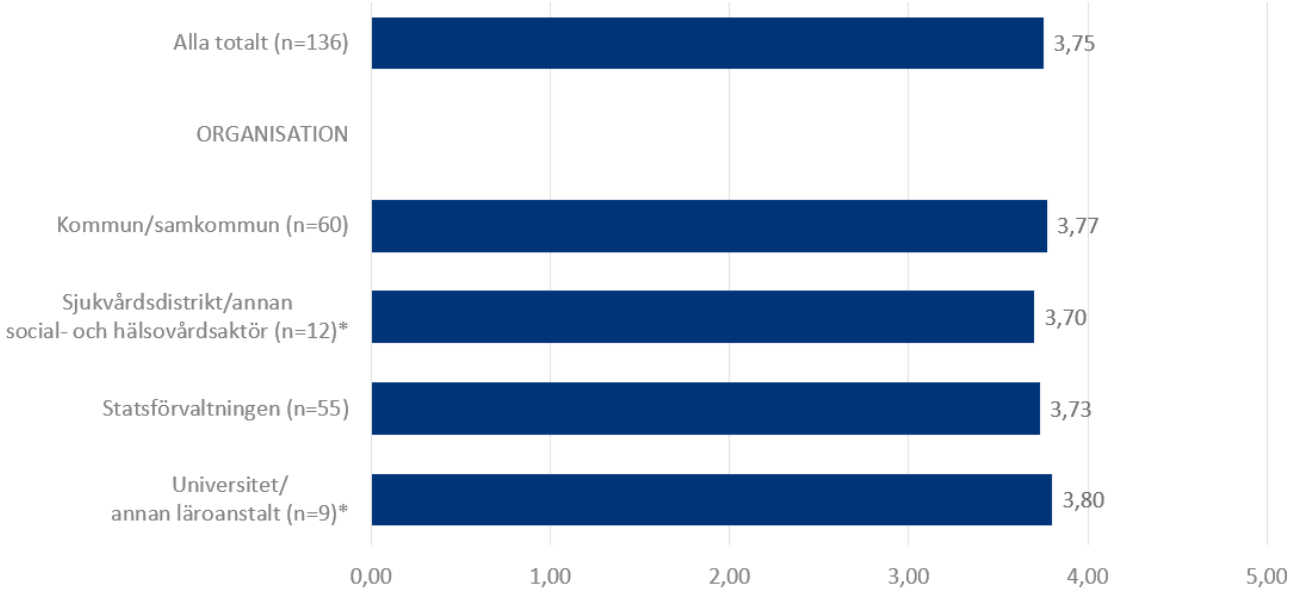

Bild 6. Diagram. Medeltal av frågorna 1–4.

Medeltalet för alla svar är 3,75, dvs. något sämre än bra. Skillnaderna mellan verksamhetsområdena är här mycket små, endast 0,05 på båda sidor om medelvärdet. Detta visar att coronaviruspandemin har visat sig vara mycket likartad för de verksamhetsområden som deltog i enkäten. I vissa frågor är skillnaderna något större, men som helhet är de mycket små.

	Alla totalt	Kommun/samkommun	Sjukvårdsdistrikt/annan social- och hälsovårdsaktör	Statsförvaltningen	Universitet/annan läroanstalt
Medeltal av punkterna 1–4 ovan	3,75	3,77	3,70	3,73	3,80

Bild 6. Texttabell. Medeltal av frågorna 1–4.

2.2 Hot som organisationerna upplever

Enkätens andra del bestod av frågor som gällde identifiering av hot och utveckling av verksamheten. Syftet med dem var att utreda hurdana verksamhetsrelaterade hot som har inträffat under våren och hur väl de har kunnat hanteras. Samtidigt ville man utreda hur organisationerna har utvecklat sin verksamhet och hur den digitala säkerheten har kunnat beaktas.

2.2.1 Realiseringen av olika hot

Organisationerna tillfrågades om hur tolv på förhand utvalda hot har realiserats i deras verksamhet. Svarsalternativen för varje hot var antingen ja eller nej. Dessutom skulle man bedöma hur många hot som har förverkligats och hur de har beaktats i riskhanteringen.

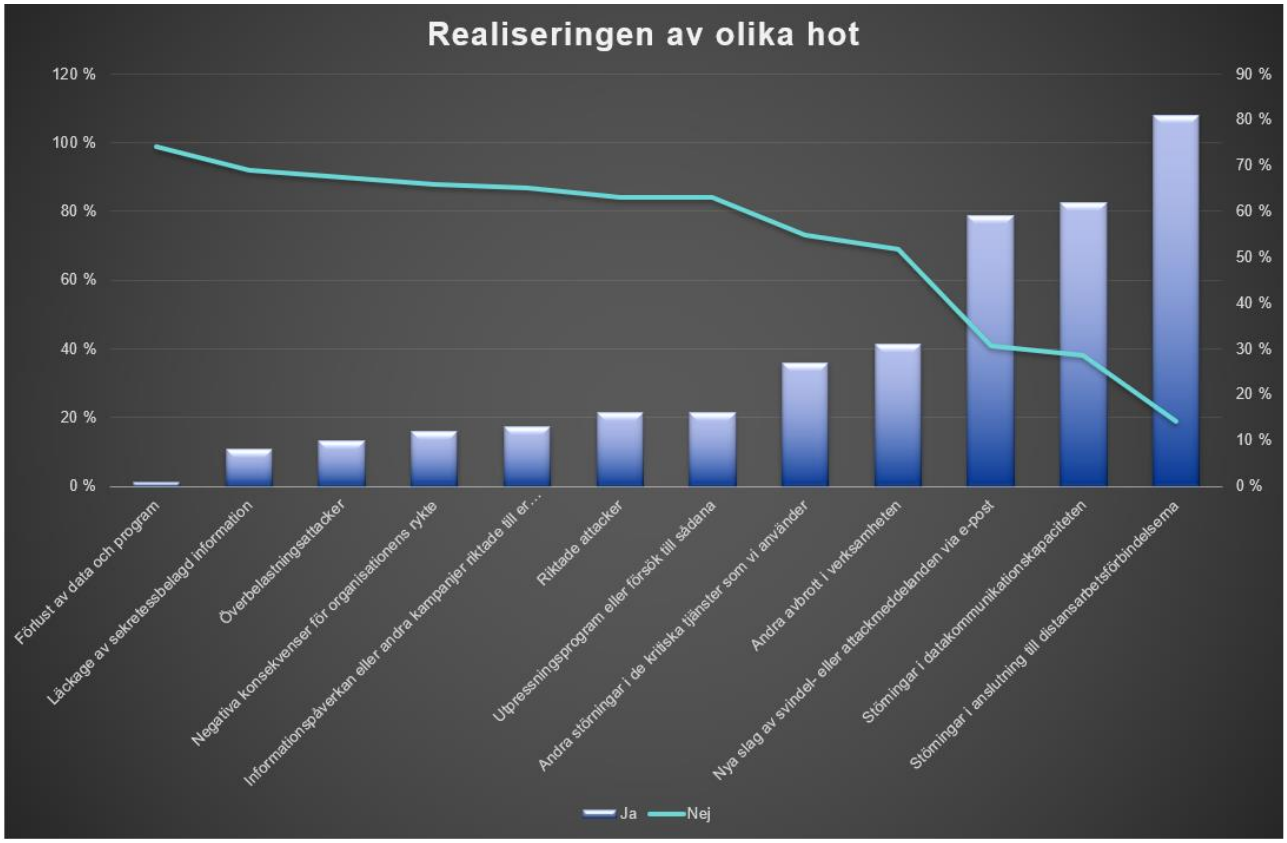

Bild 7. Diagram. De hot som respondentorganisationerna har identifierat. Den blå balken beskriver som procentandel hos hur många organisationer hotet realiserats - den orange linjen beskriver antalet organisationer hos vilka hotet inte har förverkligats.

De överlägset största problemen har orsakats av störningar i fjärrförbindelserna (81 procent). Här kan man visserligen konstatera att man efter inledningsskedet har fått bättre kontroll över problemen.

De näst största problemen har orsakats av störningar i datakommunikationskapaciteten (62 procent). Som en följd av detta har det framkommit ett behov av att begränsa eller ge anvisningar för personalens verksamhet, till exempel i användningen av VPN-tjänsten. För en del av respondenterna har detta hot realiserats i form av långsammare internationella molntjänster och överbelastning. I Finland har operatörerna som tillhandahåller datakommunikationsförbindelser däremot framgångsrikt kunnat erbjuda datakommunikationskapacitet trots en betydande ökning av belastningen.

Det tredje vanligaste hotet har varit "nya slag av svindel- eller attackmeddelanden via e-post" (59 procent). I praktiken bytte flera kriminella organisationer och nätbrottslingar snabbt ut sina befintliga bedrägerimetoder mot sådana med Covid-19- eller coronavirusteman. De lösningar för skadliga program kan i allmänhet filtrera sådana här meddelanden, i praktiken är de ett större problem för personer som använder e-post på fritiden.

De återstående nio hoten låg på mindre än 50 procent. Det lönar sig att beakta det rätt höga antalet i punkten Utpressningsprogram eller försök till sådana (16 procent). Detta antal kan delvis förklaras med att många personer får enstaka e-postmeddelanden om svindelutpressning. De hotar ofta med att publicera en snuskig video om personen, om personen inte betalar utpressaren. Naturligtvis ska organisationerna varna och instruera personalen att agera rätt i dessa situationer.

Det var positivt att notera att de minsta hoten var särskilt kritiska överbelastningsattacker (10 procent), läckage av sekretessbelagda uppgifter (8 procent) samt förlust av data och programvara (1 procent). Däremot är det oroväckande att 8 procent av organisationerna har identifierat läckage av sekretessbelagda uppgifter som ett hot. I enkäten utreddes inte vilken typ av information det är frågan om eller hur stor mängd uppgifter det gäller, så det går inte att göra en noggrannare analys av detta.

Hot	Ja	Nej
Störningar i anslutning till distansarbetsförbindelserna	81 %	19 %
Störningar i datakommunikationskapaciteten	62 %	38 %
Nya slag av svindel- eller attackmeddelanden via e-post	59 %	41 %
Andra avbrott i verksamheten	31 %	69 %
Andra störningar i de kritiska tjänster som vi använder	27 %	73 %
Riktade attacker	16 %	84 %
Utpressningsprogram eller försök till sådana	16 %	84 %

Informationspåverkan eller andra kampanjer riktade till er organisation	13 %	87 %
Negativa konsekvenser för organisationens rykte	12 %	88 %
Överbelastningsattacker	10 %	90 %
Läckage av sekretessbelagd information	8 %	92 %
Förlust av data och program	1 %	99 %

Bild 7. Texttabell. De hot som respondentorganisationerna identifierat, de oftast realiserade hoten överst och de minst realiserade nederst.

2.2.2 Genomförande av riskhantering i anslutning till hot

Organisationerna tillfrågades om hur väl de har identifierat och behärskat ovan nämnda risker. Av följande tabell framgår att riskhanteringen i huvudsak motsvarar identifieringen av realiserade risker; ju mer hotet har stört organisationens verksamhet, desto mer har man fäst uppmärksamhet vid riskhanteringen i fråga.

Riskhanteringen bedömdes på följande skala:
4 Hotet har identifierats och den risk det medför har behärskats väl
3 Hotet har identifierats och de restrisker som är förknippade med hotet är i huvudsak under kontroll
2 Hotet har identifierats men förknippas med tydliga, delvis okända och okontrollerade risker
1 Hotet har identifierats och förknippas med betydande okontrollerade risker som hotar vår verksamhet
0 Vi har inte identifierat och hanterat detta hot alls

Hot	**Riskhantering**
Störningar i anslutning till distansarbetsförbindelserna	2,88
Nya slag av svindel- eller attackmeddelanden via e-post	2,59
Störningar i datakommunikationskapaciteten	2,45
Andra avbrott i verksamheten	1,87
Andra störningar i de kritiska tjänster som vi använder	1,95
Riktade attacker	1,70

Utpressningsprogram eller försök till sådana	1,84
Informationspåverkan eller andra negativa kampanjer riktade mot er organisation	1,76
Negativa konsekvenser för organisationens rykte	1,73
Överbelastningsattacker	1,78
Läckage av sekretessbelagd information	1,76
Förlust av data och program	1,76

Bild 8. Texttabell. Respondenterna har identifierat och fått kontroll över olika hot

Av tabellen framgår att till exempel punkterna "Övriga avbrott i verksamheten", "Riktade attacker", "Negativa konsekvenser för organisationens rykte" och "Överbelastningsattacker" inte är i exakt samma ordning som de har riktats mot organisationer, men skillnaderna är inte betydande. Det viktigaste är att de tre överlägset mest störande riskerna har identifierats och uppmärksammats.

Observera!

*En del organisationer har svarat på enskilda hot genom att välja alternativ **1. Hotet har identifierats och förknippas med betydande okontrollerade risker som hotar vår verksamhet.***

Varje organisation som svarat bör gå igenom sitt svar och omvärdera vilka hanteringsåtgärder som bör vidtas för en sådan risk. Ju mer ett sådant hot har förekommit hos andra organisationer, desto viktigare är det att få kontroll över den okontrollerade risk som hotar verksamheten.

I augusti 2020 publicerar vi en uppdaterad version av denna rapport där vi behandlar olika delområden mer detaljerat. Tabellen ovan kan också tolkas på så vis att även om organisationen inte nu har identifierat riskerna i anslutning till hoten på listan, borde de kanske i fortsättningen ta bättre kontroll över dem.

När det gäller alla identifierade risker, dvs. de som angetts i svaret, är genomsnittet för riskhanteringen 3,23, vilket kan anses vara överraskande högt. Det bör dock observeras att en del av respondenterna hade identifierat endast ett eller två hot mot dem. Om dessa var väl under kontroll var svaret 4, dvs. hotet och risken som det orsakade var väl under kontroll.

De organisationer som svarat kan kontrollera i sammanfattningen i sina svarstabeller punkten ”Hur många olika hot har ni upplevt - minimum är 0 och maximum är 12 (ju högre siffra, desto mer oroande är er situation).” Tabellen nedan visar hur många hot olika organisationerna i genomsnitt har identifierat.

	Alla	Kommun/samkommuner	Sjukvårdsdistrikt/annan aktör inom social- och hälsovården	Statsförvaltningen	Universitet/Annan läroanstalt
Antal realiserade hot: Hur många olika hot har ni upplevt - minimum är 0 och maximum är 12	3,39	3,13	3,00	3,67	3,89

Bild 9. Texttabell. Hur många olika hot har organisationerna identifierat i genomsnitt per verksamhetsområde.

Flest hot har identifierats av universitet och andra läroanstalter (3,89 st./organisation) och på motsvarande sätt har sjukvårdsdistrikten och andra aktörer inom social- och hälsovården identifierat minst hot (3 st./organisation) när medelvärdet är 3,39.

2.2.3 De realiserade hotens omfattning/hot

De organisationer som svarat kan kontrollera omfattningen av de realiserade hoten under sammandraget i svarstabellen. Se punkt ”De realiserade hotens omfattning: Hur många olika hot har ni utsatts för kvantitativt ". Tabellen nedan visar hur många olika hot som har realiserats inom de olika verksamhetsområdena.

Organisationerna valde för varje konstaterat hot antalet sådana. Svaren poängsattes enligt följande:
Inte alls 0 poäng
Enstaka/få 1 poäng
I viss mån 2 poäng
I hög grad 3 poäng
Mycket 4 poäng

Av dessa har man beräknat ett jämförelsetal som är desto större ju fler hot som har realiserats hos organisationen.

	Alla	Kommun/samkommuner	Sjukvårdsdistrikt/annan aktör inom social- och hälsovården	Statsförvaltningen	Universitet/Annan läroanstalt
De realiserade hotens omfattning: Hur många olika hot har ni upplevt kvantitativt - minimum är 0 och maximum är 48	5,02	4,40	4,50	5,78	5,22

Bild 10. Texttabell. Hur många olika hot har kvantitativt realiserats inom organisationerna.

Medeltalet för jämförelsetalet är 5,02. Det största antalet identifierade hot finns inom statsförvaltningen, på motsvarande sätt har kommunerna och samkommunerna det minsta antalet identifierade hot.

I detta sammanhang lönar det sig att särskilt nämna att största delen av svaren som gällde antalet faktiska hot var svaret enstaka/få eller i viss mån. Endast några organisationer hade observerat dessa i betydande grad vid ett enskilt hot och alternativet mycket hade valts i endast ett svar.

Detta illustreras också av att när punktens medelvärde 5,02 divideras med medeltalet för de faktiska hoten på 3,39 blir värdet 1,48 - detta värde ligger mellan enstaka/få och i viss mån.

Kvantitativt flest problem låg hos de oftast realiserade hoten, dvs.:

- Störningar i anslutning till distansarbetsförbindelserna
- Nya slag av svindel- eller attackmeddelanden via e-post
- Störningar i datakommunikationskapaciteten

2.2.4 Att göra hoten en del av riskhanteringen

De organisationer som svarat kan kontrollera omfattningen av de realiserade hoten under sammandraget i svarstabellen. Se punkt ”Hur har er riskhantering kunnat hantera dessa hot?” I det här avsnittet beskrivs hur väl organisationerna i genomsnitt har hanterat hoten.

Organisationernas bedömningar av riskhanteringsnivån för vart och ett av de 12 hoten har poängsatts enligt följande:
4 Hotet har identifierats och den risk det medför har behärskats väl 0 poäng
3 Hotet har identifierats och de restrisker som är förknippade med hotet är i huvudsak under kontroll 1 poäng
2 Hotet har identifierats men förknippas med tydliga, delvis okända och okontrollerade risker 2 poäng
1 Hotet har identifierats och förknippas med betydande okontrollerade risker som hotar vår verksamhet 3 poäng
0 Vi har inte identifierat och hanterat detta hot alls

Jämförelsetalet är minst 0 poäng och maximalt 36 poäng, ju färre poäng, desto bättre har hoten kunnat kontrolleras.

	Alla	Kommun/samkommuner	Sjukvårdsdistrikt/annan aktör inom social-	Statsförvaltningen	Universitet/Annan läroanstalt

			och hälsovården		
Identifiering och hantering av hot: Hur har er riskhantering fått dessa hot under kontroll?	6,67	6,50	7,17	5,80	12,44

Bild 11. Texttabell. Hur har man lyckats hantera hoten i riskhanteringen?

Svaret är i genomsnitt 6,67. Statsförvaltningen (5,80) får det minsta poängantalet, endast universiteten och andra läroanstalter avviker avsevärt från genomsnittet. Vid bedömningen av svaren bör man observera att värdet också påverkas av att alla respondenter inte har identifierat och behandlat alla hot och att det finns betydande skillnader mellan de olika respondenterna.

2.3 Utveckling av verksamheten i en förändrad verksamhetsmiljö

De två sista frågorna i enkäten gällde hur organisationen eventuellt har ändrat sina verksamhetsprinciper för digital säkerhet i en förändrad verksamhetsmiljö.

2.3.1 Ändring av processer och verksamhetsmodeller som gäller säkerheten

De organisationer som svarat kan i sina svarstabeller på fliken Sammanfattningssvar kontrollera punkten "Hur mycket har ni varit tvungna att ändra era befintliga processer och säkerhetsrelaterade verksamhetsmodeller?".

Här frågade vi följande:

Utveckling av verksamheten och möjliggörande av den i en förändrad verksamhetsmiljö

A) Vi har tagit i bruk nya processer eller tjänster utan tillräcklig riskhantering ELLER
B) Vi har inte prutat på riskhanteringen trots att vi har tagit i bruk nya processer eller tjänster ELLER
C) både och

A) Vi har tagit i bruk nya verktyg eller tjänster utan ett tillräckligt säkerhetstest ELLER
B) Vi har tagit i bruk nya verktyg eller tjänster efter tillräcklig säkerhetstestning ELLER
C) både och

A) Vi har försvagat säkerhetsprocesserna för att möjliggöra tillgången till tjänster ELLER
B) Vi har inte försvagat säkerhetsprocesserna för att möjliggöra tillgången till tjänster ELLER
C) både och

A) Personalen har i distansarbete kunnat hantera sådant material som det inte tidigare varit tillåtet att hantera ELLER
B) Personalen har inte kunnat hantera sådant material i distansarbete som det inte heller tidigare varit tillåtet att hantera ELLER
C) både och

A) Anvisningarna och utbildningen för personalen i den förändrade situationen har varit bristfällig ELLER
B) Anvisningarna och utbildningen för personalen i den förändrade situationen har varit tillräcklig ELLER
C) både och

A) Vi har varit tvungna att försvaga processerna för behandling av personuppgifter ELELR b) Vi har inte varit tvungna att försvaga processerna för behandling av personuppgifter ELLER
C) både och

Det första svarsalternativet gav 4 poäng, det andra 0 poäng och det tredje 2 poäng. Det totala poängantalet är 0 (man har inte alls prutat på säkerheten) och maximiantalet är 24 (man har varit tvungen att ändra processerna i betydande grad).

I svaren var det högsta poängantalet för en enskild organisation 16 poäng, men cirka 20 organisationer fick 10 eller fler poäng. Det minsta poängantalet var 2, och två respondenter fick det antalet.

	Alla	Kommun/samkommuner	Sjukvårdsdistrikt/annan aktör inom social- och hälsovården	Statsförvaltningen	Universitet/Annan läroanstalt
Hur mycket har ni tvingats ändra på era befintliga processer och säkerhetsrelaterade verksamhetsmodeller?	5,07	4,88	4,33	5,33	5,78

Bild 12. Texttabell. Hur mycket har ni tvingats ändra på era befintliga processer och säkerhetsrelaterade verksamhetsmodeller?

Medeltalet för alla respondenter är 5,07. Sjukvårdsdistrikten och andra aktörer inom social- och hälsovården har det minsta medelvärdet (4,33), och på motsvarande sätt har universiteten och andra läroanstalter högst medelvärde (5,78). Ju mer kompromisser eller försämringar organisationen har tvingats göra i befintliga verksamhetsmodeller eller processer för digital säkerhet, desto noggrannare ska organisationen säkerställa säkerheten i sin verksamhet och sina uppgifter samt dataskyddet när den återvänder till den normala situationen.

2.3.2 Förändringarnas omfattning

De organisationer som svarat kan i sina svarstabeller på fliken Sammanfattningssvar kontrollera punkten "Hur mycket har ni varit tvungna att ändra era befintliga processer och säkerhetsrelaterade verksamhetsmodeller?". I det här avsnittet har man jämfört i vilken omfattning organisationen har varit tvungen att genomföra dessa förändringar i sin verksamhet.

Svaren har getts på följande skala:

- Inte alls
- Enstaka/få
- I viss mån
- I hög grad
- Mycket

I tabellen finns ett jämförelsetal som baserar sig på det alternativ som valts i föregående punkt samt på ändringens omfattning. Om organisationen till exempel har tagit i bruk "nya processer eller tjänster utan tillräcklig riskhantering" och detta har skett ”Mycket” får organisationen 16 poäng. På motsvarande sätt, om organisationen har svarat "Vi har inte försvagat säkerhetsprocesserna för att möjliggöra tillgången till tjänster", får organisationen 0 poäng.

Detta jämförelsetal har ett minimum på 0 (säkerheten har inte alls eller i ytterst liten utsträckning varit tvungen att försämras) och maximivärdet är 96 (många säkerhetsförsämringar har varit tvungna att genomföras).

	Alla	Kommun/samkommuner	Sjukvårdsdistrikt/annan aktör inom social- och hälsovården	Statsförvaltningen	Universitet/Annan läroanstalt
I vilken omfattning har ni tvingats genomföra dessa förändringar?	4,44	3,93	4,50	4,75	5,89

Bild 13. Texttabell. I vilken omfattning organisationen har varit tvungen att genomföra dessa förändringar.

Även om skalan i denna fråga är bredare än i andra, hålls medeltalet på en måttlig nivå (4,44). I denna punkt får kommunerna och samkommunerna det minsta jämförelsetalet och universiteten och de övriga läroanstalterna det största (5,89). Skillnaderna mellan branscherna kan anses vara små.

Totalt får cirka 15 organisationer här ett högre värde än 10 och två organisationer ett värde över 30.

Även med hjälp av denna fråga har man väckt organisationerna till att bedöma hurdana förändringar i den digitala säkerheten de har gjort och vilka konsekvenser de kan ha för organisationens säkerhet. Ändringarna ska vara antecknade och riskerna i anslutning till dem bedömda så att man vid återgång till normala förhållanden kan försäkra sig om att verksamhetens säkerhet och tillförlitlighet återställs till minst den nivå som rådde före koronaviruspandemin.

2.4 Öppna frågor

2.4.1 Önskad hjälp från VAHTI-verksamheten eller andra myndigheter

I slutet av enkäten fanns två öppna frågor, varav den första var frågan "Vilken typ av hjälp önskar ni av VAHTI-verksamheten eller andra myndigheter i denna situation eller för att möjliggöra återhämtning samt för att trygga säkerhet och förtroende?"

Vi fick 49 svar på detta. Några av de viktigaste önskemålen kommer att sammanfattas i ordmolnet nedan.

Organisationerna förväntar sig inte någon egentlig hjälp för att sköta coronaviruspandemin, eftersom situationen upplevs som under kontroll, men som sammanfattning framkommer följande förslag:

- utvärdering av verktyg och mobila lösningar för distansarbete, bedömning av informationssäkerheten för molntjänster (i allmänhet objektiv bedömning av säkerheten hos de tjänster som används)
- ytterligare anvisningar och utbildning för olika delområden inom digital säkerhet
- lägesbildsrapportering
- säkerställande av att datakommunikationskapaciteten är tillräcklig
- nätverksbaserat arbete för samarbetet och spridande av bästa praxis
- för övningar och situationer som motsvarar övningar
- anvisningar och riktlinjer för användningen av molntjänster
- gemensam riskrapportering och scenarier
- en fredning under krisarbetet - bort med allt onödigt
- utveckling av kompetensen och medvetenheten hos organisationens ledning
- stöd för identifiering av kritiska tjänster och processer

- VAHTI kunde samla allt vi lärt oss av coronaviruset

Här följer tre önskemål som plockats ur svaren:

- "VAHTI-arbetet borde koncentreras till att täcka och hantera 80 procent av riskerna med 20 procent av organisationernas resurser. Resten blir restrisker och det lönar sig inte att sätta resurser för dem. ”

- "Sammanfattning av hurdana fall av cybersäkerhet som observerats i Finland under pandemin och hur de har avvärjts/utretts.”

- "Allmänna och lättförståeliga anvisningar för distansarbete (personal + förtroendevalda).”

Både i detta svar och i en del av de tidigare frågorna lyftes det stöd och det material som Cybersäkerhetscentret vid Transport- och kommunikationsverket producerat samt övrig kommunikation fram, inte bara nu när det gäller att hantera coronaviruspandemin utan mer allmänt i utvecklingen av informations- och cybersäkerheten.

2.4.2 Kommentarer, idéer och respons

Till sist fick vi 36 andra kommentarer. Responsen berömde och ansåg att enkäten var nödvändig. De sista frågorna fick flest utvecklingsförslag eftersom de inte innehöll alla svarsalternativ som svarsorganisationen önskade. Likaså kom respons om att de skalor som används i alla frågor bör vara enhetliga. Dessutom önskade man att enkäten kunde besvaras via den elektroniska tjänsten.

Dessa respons beaktas när man i Myndigheten för digitalisering och befolkningsdatas JUDO-projekt utvecklar en helhetsbildtjänst för digital säkerhet, med vars hjälp sådana enkäter kan genomföras i fortsättningen.

Här följer tre kommentarer som plockats ur svaren:

"Tack för enkäten, bra att dessa frågor sammanställs. Det var givande att fylla i den i expertgruppen. ”

"Som kommunal aktör är det svårt att fylla i denna tabell eftersom verksamheten är så omfattande.”

"Responsen är i sig till nytta för organisationen och vi använder denna blankett för egen uppföljning. Sammanställningen av svaren och den interna behandlingen hjälpte den högsta ledningen att informera om frågor som gäller digital säkerhet i lämplig form, även om vårens alla övriga stress och bekymmer har belastat ledningen och den digitala tryggheten i sig inte har varit den högsta ledningens bekymmer i coronasituationen. ”