Myndigheten för digitalisering och befolkningsdata 8.10.2020

TAISTO20 -övningshandbok

Anvisningar för organisationer som förbereder sig inför TAISTO20-övningen

8.10.2020

Innehållsförteckning

TAISTO20-övningshandbok

TAISTO-övningen är en övning i hantering av dataskydds- och datasäkerhetskränkningar som riktar sig till den offentliga förvaltningen. I övningen övar organisationerna på verksamhetsmodeller och processer för olika störningssituationer. Med hjälp av övningen kan reaktionen på en kränkning av datasäkerheten eller dataskyddet skötas mer kontrollerat i en verklig situation, varvid återhämtningen blir snabbare.

Myndigheten för digitalisering och befolkningsdata ansvarar för genomförandet och styrningen av TAISTO-övningen. Ledare för övningen är Hanna Heikkinen, datasäkerhetsexpert vid Myndigheten för digitalisering och befolkningsdata. I genomförandet av övningen deltar dessutom Laura Penttilä, sakkunnig vid Myndigheten för digitalisering och befolkningsdata. Övningen planeras i samarbete med Centralkriminalpolisen, Cybersäkerhetscentret, dataombudsmannens byrå, Valtori och Säkerhetskommittén.

Efter TAISTO20-övningarna som hålls i oktober och november publicerar Myndigheten för digitalisering och befolkningsdata övningsmaterialet så att det är tillgängligt för alla. Vi hoppas att deltagarna i TAISTO20-övningen inte offentligt delar material om övningens innehåll innan dess.

Målen med TAISTO20-övningen är att

- Identifiera olika myndigheters uppgifter i olika situationer.
- Utveckla hanteringen av datasäkerheten, ledningen och kommunikationen i störningssituationer.
- Utveckla de processer som behövs vid kränkningar av dataskyddet, såsom förmågan att bedöma den uppkomna risken, göra nödvändiga anmälningar till myndigheter, intressentgrupper och registrerade.
- Utveckla anvisningar och verksamhetsprocesser för verksamhetens kontinuitet, beredskap och kommunikation i störningssituationer.

Organisationerna bör gå igenom målen för TAISTO20-övningen med praktikgruppen före övningen. Dessutom kan organisationen om den så önskar lägga till egna mål för övningen TAISTO20 utöver de allmänna målen.

1 Förberedelse inför övningen

Tyngdpunkten i övningen ligger på att utveckla organisationens egna processer, anvisningar och verksamhetsmodeller.

- Se till att organisationen har uppdaterade processer och anvisningar för kränkningar av dataskyddet. Dessutom är det bra om organisationen för övningen har planer och anvisningar för kontinuitet och beredskap, enligt vilka man agerar i olika störnings- och undantagssituationer.

Kontaktpersonen för organisationens övning ansvarar för att organisationen har lämpliga kommunikationsmedel och lokaler för övningen.

- Kom ihåg att göra nödvändiga reserveringar i kalendern även för organisationens övningsgrupp.

Observera att personer med olika roller som har ansvar för att hantera störningar och avvikelser och trygga kontinuiteten ska delta i övningen. Dessa roller är bland annat ledningens representant, datasäkerhetsansvarig, dataskyddsombud, kommunikationsexpert samt ICT-expert.

- Det lönar sig för en person att ha endast en roll i övningen så att övningen löper smidigt. Det är bra att gå igenom rollerna på övningsdagens morgon så att alla förstår sin roll/uppgift i övningen.

Vi rekommenderar att organisationen inför en observatör som dokumenterar dagens händelser och observationer.

- Det lönar sig att koppla in en utomstående observatör till övningsdagen så att organisationen får största möjliga nytta av övningen. Han eller hon antecknar objektivt observationer om organisationens verksamhet i anslutning till situationen.

- En anvisning för observatören och en blankett för observationer publiceras vecka 42 på adressen www.dvv.fi/taisto

I år används övningsplattformen Trasim för att förmedla övningens händelser, flöden och medielägesbilden som motsvarar världsbilden. Övningsdagen består av händelser och tillhörande meddelanden. Meddelandena publiceras enligt tidtabellen på övningsplattformen.

- Observera att inget separat e-postmeddelande/påminnelse skickas om meddelandena.

- Om du får problem med övningsplattformen under övningsdagen ska du omedelbart skicka e-post till adressen digiturva@dvv.fi med rubriken: TAISTO20-övningen: problem med övningsplattformen

I övningen undersöks inte närmare orsakerna till en eventuell informationssäkerhetsincident, attack eller personuppgiftsincident, och inte heller görs någon noggrannare utredning av det inträffade (forensik). Organisationen ska som en del av de fortsatta åtgärderna inom ramen för övningen och för att utveckla den egna verksamheten utreda och bedöma hur den skulle fortsätta den nödvändiga utredningen av situationen i en situation lik övningen.

Organisationen kan om den så önskar använda till exempel serviceproducenter i övningen. Organisationen ska själv avtala om användningen av dessa. Myndigheten för digitalisering och befolkningsdata ansvarar inte för att dessa parter deltar i övningen eller för kostnader i anslutning till övningarna. Tjänsteleverantörerna fakturerar er för detta arbete enligt ert gällande avtal.

Under övningsdagen ska organisationen agera på samma sätt som i en riktig situation. Organisationen ska genomföra intern kontakt, e-postmeddelanden, diskussioner via snabbmeddelanden, eventuella meddelanden och andra åtgärder som den skulle göra i en verklig situation. Kom ihåg att skriva TAISTO20-ÖVNING i alla meddelanden så att ingen tror att situationen är på riktigt.

2 Skärmansvariga

Organisationerna har två utsedda skärmansvariga på övningen. De skärmansvariga har i uppgift att dela kontrollvyn för övningsplattformen och de meddelanden som publicerats i den till organisationens övningsgrupp. De ansvariga delar den egna skärmen (vyn för övningsplattformen) vid ett virtuellt möte som organisationen själv ordnar eller på motsvarande sätt i ett fysiskt rum, såsom ett mötesrum. De skärmansvariga måste delta i övningen. Kontaktpersonen för organisationens övning ansvarar för att organisationen har lämpliga kommunikationsmedel och lokaler för övningen.

De skärmansvariga får anvisningar om hur man aktiverar användarkontot och fungerar som skärmansvarig under övningen. De skärmansvariga har fått som förhandsuppgift att logga in på övningsplattformen och säkerställa att koderna fungerar.

Anvisningar för att fungera som skärmansvarig under övningen och logga in på övningsplattformen finns på www.dvv.fi/taisto.

3 Förhandsuppgifter

Till alla organisationer som övar

- Se till att organisationen har nödvändiga processer och anvisningar för personuppgiftsincidenter.
- Se till att organisationen har planer och anvisningar gällande kontinuitet och beredskap, enligt vilka man agerar vid störningar, avvikelser och situationer av kränkning som riktas mot organisationen.
- Se till att organisationen har en process för att göra myndighetsanmälningar (informationssäkerhets- och dataskyddsintrång).
- Vi rekommenderar att du bekantar dig med utbildningen Trygga den digitala verksamheten i störningssituationer. Utbildningen finns på finska på adressen: https://www.eoppiva.fi/kurssit/turvaa-digitaalinen-toiminta-hairiotilanteissa/#/. Utbildningen hjälper organisationen att förbereda sig för övningen.

Vi rekommenderar att man säkerställer att organisationen har förmåga att

- Agera vid personuppgiftsincidenter, som att bedöma riskerna för den registrerades rättigheter och friheter.
- Agera i en situation där organisationens personuppgifter har hamnat hos utomstående aktörer.

- Konstatera att dataintrång och/eller personuppgiftsincidenter har skett i de tjänster som den använder.
- Börja leda situationen.
- Bedöma hur stora de realiserade riskerna är.
- Göra anmälningar till myndigheter och registrerade.
    - gällande kränkningar av datasäkerheten till Transport- och kommunikationsverkets Cybersäkerhetscenter.
    - gällande polisanmälan till Polisen.
    - gällande personuppgiftsincident till dataombudsmannens byrå.
    - anmälningar till registrerade.

Organisationer som deltar i en heldagsövning

Eftermiddagen börjar med att en person som är avgörande för organisationen tas åt sidan från övningen. Temat för eftermiddagens övningsdel är utnyttjande av sårbarheter och betalningsrörelse. Vi rekommenderar att man väljer en person från dessa roller. Alternativen för att flytta en person är:

1. Personen övergår till att granska övningsgruppens verksamhet med tanke på hur funktionerna organiseras och uppgifterna kan utföras när rollen i fråga inte används för skötseln av uppgifterna. Personen i fråga får inte delta i diskussionen eller ge råd.
    - Har man gett tillräckligt med instruktioner och utbildning om uppgifterna som ingår i rollen för att uppgifterna ska kunna skötas under övningen?
    - Personen följer med övningsgruppens verksamhet och gör observationer som gäller uppgifter inom hans eller hennes ansvarsområde och utformar utvecklingsåtgärder utgående från dessa.
2. Personen befrias helt från övningen.

Vi rekommenderar alternativ ett, vilket ger organisationen mer nytta av övningen.

4 Övningsdagen

Kontrollera i god tid på övningsdagens morgon att den skärmansvariga kan logga in på övningsplattformen och dela skärmen med organisationens övningsgrupp. Kontrollera i början av övningen att de personer som kallats till övningsgruppen är på plats antingen vid organisationens eget virtuella möte eller fysiskt i konferensrummet.

Övningsdagen börjar med en hälsning som publiceras på övningsplattformen. Dessutom kommer på övningsplattformen publiceras korta informationsanslag från Cybersäkerhetscentret, Centralkriminalpolisen och Dataombudsmannens byrå om hur man gör ett myndighetens meddelande. Nyhetsöversikter på träningsplattformen öppnar

övningens världsbild. Vi ber att organisationens övningsgrupp tittar dessa noga igenom i början av övningsdagen. Total varaktighet för videor är under 10 minuter.

I övningen modelleras situationer där många saker redan har gått fel. På så sätt kan organisationen samtidigt öva på flera saker som eventuellt dyker upp. Övningsdagen består av olika händelser, meddelanden och uppgifter. Meddelandena publiceras enligt tidtabellen på övningsplattformen. Observera att inget separat e-postmeddelande/påminnelse skickas om meddelandena, utan all verksamhet sker på övningsplattformen.

I övningen användes en övningsplattform för första gången för att förmedla en mediasituationsbild som motsvarar övningens världsbild. Medieflöden visas till höger i vyn på övningsplattform, under vilken ett kommentarsfält visas. Om du lägger till en kommentar i kommentarsfältet visas den för alla organisationer som deltar i övningen. Av denna anledning ber vi att inte lägga upp dina egna kommentarer i kommentarsfältet under övningen.

Det lönar sig att komma till övningen med ett positivt och öppet sinne. TAISTO-övningens målgrupp är omfattande och därför har man försökt beskriva händelser och meddelanden så generiskt som möjligt. Vi hoppas att de som deltar i övningen inte spelar mot "spelet", det vill säga letar efter fel i meddelandena som gör att man kan förbigå händelser och meddelanden. Dessutom lönar det sig att vara lika realistisk i övningssituationen som i verkligheten, så att organisationen får ut så mycket som möjligt av övningen.

Vi rekommenderar att organisationen för övningsdagbok på övningsdagen. I övningsdagboken antecknas observationer och åtgärder som vidtagits under övningen. Under övningen ska ni genast anteckna sådana observationer som kräver att ni utvecklar anvisningarna eller handlingsprocesserna. Det hjälper organisationen att efter övningen återgå till övningsdagens händelser, analysera den egna verksamheten under övningen och sammanställa de utvecklingsåtgärder som presenterats under övningen. Organisationen kan om den så önskar under övningsdagen använda TAISTO20-övningsdagboken för att följa upp den egna verksamheten och rapportera genomförda åtgärder. Dagboken finns på adressen www.dvv.fi/taisto.

Organisationen har i samband med anmälan valt hur lång övningsdagen ska vara, halvdag eller heldag, enligt egna behov. Övningsdagens längd bestäms enligt valet, för en del organisationer avslutas övningen klockan 12, varefter organisationen utför den fastställda efterbehandlingen. Heldagsövningen fortsätter kl. 12.30 och avslutas kl. 15.00, varefter de organisationer som deltar i heldagen genomför efterbehandling. Observera att klockan 12.00 börjar en halvtimmes paus för deltagarna i heldagsövningen.

Övningsdagens förlopp

9.00 Övningsdagen börjar på övningsplattformen
- Händelse 1 och tillhörande meddelanden
- Händelse 2 och tillhörande meddelanden
- Händelse 3 och tillhörande meddelanden
- Händelse 4 och tillhörande meddelanden

12.00 Halvdagen avslutas
- Efterbehandling för dem som avslutat en halvdagsövning

12.30 Heldagen fortsätter
- Händelse 5 och tillhörande meddelanden
- Händelse 6 och tillhörande meddelanden
- Händelse 7 och tillhörande meddelanden
- Händelse 8 och tillhörande meddelanden

15.00 heldagsrepetitionen avslutas
- Åtgärder efter avslutad övningsdag

Myndighetsanmälningar i övningen

Alla myndighetsanmälningar i TAISTO20-övningen görs via övningsplattformen. Anvisningar och länkar till myndighetsanmälningar finns på övningsplattformen. Vi önskar att organisationerna tar ett aktivt grepp om att göra myndighetsanmälningar under TAISTO20-övningen. Observera att man inte tar kontakt med myndigheterna som i en verklig situation, utan all kontakt under övningen sker via övningsplattformen.

Myndighetsanmälningarna från Centralkriminalpolisen och dataombudsmannens byrå görs på webropol-blanketter på övningsplattformen under TAISTO20-övningen. Blanketterna har modellerats utifrån riktiga myndighetsanmälningar. Efter att blanketten för myndighetsanmälan har fyllts i får organisationen information om att anmälan har mottagits från myndigheten i fråga på webropol-blanketten. Där beskrivs de första stegen i hur processen inleds hos myndigheten i fråga. Efter TAISTO20-övningen skickas sammanställningsrapporterna om myndighetsanmälningar som gjorts under övningen till myndigheten i fråga för analys.

För Cybersäkerhetscentrets del leder länken på övningsplattformen direkt till Cybersäkerhetscentrets webropol-blankett, via vilken anmälningar om kränkningar av dataskyddet görs till dem. Detta förfarande beskriver deras övningsjour.

5 Efter övningen

Som avslutning på övningsdagen får varje deltagare svara på en Menti-enkät om hur övningsdagen kändes. Menti-enkäten finns på adressen www.menti.com. Koden som används i Menti publiceras på övningsplattformen på övningsdagen.

Efter Menti-enkäten går ni igenom dagens händelser med övningsgruppen, hur övningen lyckades, vad som gick bra och vad som behöver förbättras. På så sätt får organisationen de första observationerna om hur övningen gick och allas röster blir hörda.

Efter övningen ombeds organisationens kontaktperson, eller en person som organisationen utsett, svara på respons- och rapporteringsenkäten som Myndigheten för digitalisering och befolkningsdata skickat. Syftet med responsen och rapporteringen är att mäta övningens framgång och genomslagskraft samt förtydliga målen för kommande års TAISTO-övningar så att de motsvarar organisationernas behov och

förväntningar. Vi hoppas att organisationerna aktivt ger respons om genomförandet av övningen, vi behöver både positiv och konstruktiv respons.

Närmare anvisningar för respons och rapportering publiceras före den första övningsdagen www.dvv.fi/taisto.

Dessutom är det särskilt viktigt att organisationen efter övningen går igenom de observationer som gjorts under övningen och utifrån dem planerar nödvändiga utvecklingsåtgärder. Organisationerna ska utarbeta en realistisk tidtabell för åtgärdsförslagen, utreda resursbehoven och utse ansvarspersoner. I de flesta organisationer kräver detta att utvecklingsåtgärderna godkänns enligt organisationens ledningssystem.

6 Övriga ärenden

I år pågår en bildtävling under TAISTO20-övningen. Bildtävlingen är frivillig. Publicera en eller flera bilder i anslutning till TAISTO20-övningen med en lämplig hälsning på Twitter! Bland de tweets som publicerats under övningsdagen lottar vi ut priser. Kom ihåg att lägga till hashtaggen #TAISTO20 för att vara med i utlottningen.

Kom ihåg att kommunicera i er egen organisation och t.ex. i sociala medier om TAISTO20-övningsdagen och deltagandet i den. Använd #TAISTO20 i publikationer och observera att det av publikationerna också ska framgå att det är fråga om en övning.

Myndigheten för digitalisering och befolkningsdata ordnar ett seminarium om TAISTO20-respons- och övningsverksamheten den 27 januari 2021. Anteckna datumet i kalendern. Vi skickar inbjudan till mötet till kontaktpersonerna.

7 Kontakt under övningsdagen

I problemsituationer som gäller övningens förlopp, händelser eller meddelanden under övningsdagen ska du omedelbart ta kontakt per e-post på digiturva@dvv.fi med rubriken **TAISTO20-övningen: 29.10 / 12.11 / 19.11 problem under övningen.**

Om det är fråga om ett tekniskt problem i anslutning till övningsplattformen under övningsdagen ska du omedelbart skicka e-post till adressen digiturva@dvv.fi med rubriken: **TAISTO20-övning: Teknisk störning på övningsplattformen.**

Mer information om TAISTO20-övningen finns på adressen https://dvv.fi/taisto eller så kan du fråga per e-post på adressen digiturva@dvv.fi.