MYNDIGHETEN FÖR DIGITALISERING OCH BEFOLKNINGSDATA

Taisto-övning 2023

Manuskript

14.12.2023

Tel. **0295 536 000** (växel) | Kontaktuppgifter, se **www.dvv.fi/sv**

Innehållsförteckning

Taisto-övning 2023

Manuskriptet innehåller de uppgifter som ska föras in på övningsplattformen för Taisto-övningen 2023.

1 Förhandsmaterial

På övningsplattformen publiceras förhandsanvisningar före övningen. Samma förhandsanvisningar publiceras också på adressen dvv.fi/taisto.

1.1 Förhandsanvisningar

Information om övningen: Anvisning till den som gör Taisto-övningens myndighetsanmälningar

I Taisto-övningen är du den person som gör din organisations myndighetsanmälningar och din uppgift är att göra nödvändiga myndighetsanmälningar till polisen, dataombudsmannens byrå samt Cybersäkerhetscentret.

I Taisto-övningen kontaktas inte myndigheterna på samma sätt som i verkliga situationer, utan alla anmälningar sker med nät-blanketter på övningsplattformen. Dessa blanketter motsvarar polisens, dataombudsmannens byrås och Cybersäkerhetscentrets äkta myndighetsanmälningar.

Efter Taisto-övningen skickar vi en sammanfattande rapport över myndighetsanmälningarna som gjorts på övningsdagen till varje myndighetsinstans för analys. Din organisation får dock inte separat feedback på sina anmälningar, utan syftet med förfarandet är att utveckla myndighetsverksamheten.

Anvisningar och länkar till myndighetsanmälningar finns på övningsplattformen.

Kom ihåg att ditt användarnamn är personligt och att du kan logga in på övningsplattformen endast från en enhet åt gången. Annars låses användarnamnet.

Information om övningen: Anvisning till den kommunikationsansvariga för Taisto-övningen

I Taisto-övningen är du organisationens kommunikationsansvariga och din uppgift är att utarbeta interna och externa meddelanden på samma sätt som vid verkliga störnings- eller undantagssituationer. Om ert övningsteam har en observatör och/eller en

kommunikationsobservatör, kom ihåg att dela allt kommunikationsinnehåll du utarbetat under övningen även med dem.

Du kan publicera "Quacker-uppdateringar" som motsvarar din organisations externa meddelanden och publikationer på sociala medier direkt på övningsplattformen. Följ den separata publikationsanvisningen, dvs. publicera allt externt innehåll på sidan "Taisto – Organisationens externa kommunikation". Observera att man på övningsplattformen endast kan publicera material med kommunikationsansvarigas användarnamn och att alla organisationer som deltar i övningen kan se de inlägg som görs på övningsplattformen.

Din organisations interna meddelanden ska inte publiceras på övningsplattformen, utan de utarbetas med organisationens egna arbetsredskap och hanteras internt.

Om du felaktigt publicerar organisationens interna kommunikation på övningsplattformen, vänligen kontakta taisto@dvv.fi omedelbart och rubricera ditt meddelande "Borttagande av publikation i Taisto-övningen".

Kom ihåg att ditt användarnamn är personligt och att du kan logga in på övningsplattformen endast från en enhet åt gången. Annars låses användarnamnet.

Information om övningen: Anvisning till den skärmansvariga för Taisto-övningen

I Taisto-övningen är du skärmansvarig och din uppgift är att dela övningsplattformens vy med det övriga övningsteamet. Du kan dela övningsplattformens vy på din egen skärm antingen i det fysiska mötesrummet eller genom skärmdelning på det virtuella mötet.

När du delar videor på övningsplattformen ska du beakta följande:

När du vill dela videoljudet via Teams, klicka på "Dela innehållet" och kryssa för "Inkludera datorns ljud"

I Skype kan videoljudet inte delas, utan det lönar sig att dela videorna som länkar till övningsteamet. ”Kopiera länk” finns uppe till höger i varje video. Alla videor på övningsplattformen finns på YouTube, så videorna kräver inte användarrättigheter till övningsplattformen för att fungera.

I problemsituationer som gäller övningsplattformen ber vi dig kontakta oss omedelbart per e-post taisto@dvv.fi och rubricera ditt meddelande ”Taisto-övning teknisk störning”.

Kom ihåg att ditt användarnamn är personligt och att du kan logga in på övningsplattformen endast från en enhet åt gången. Annars låses användarnamnet.

Informationsinslag

Centralkriminalpolisen: https://youtu.be/QrQ8QTgvzzI

Transport- och kommunikationsverket Cybersäkerhetscentret: https://youtu.be/QyAsC0fJCSk

Information om övningen: Förberedelser inför övningen

I Taisto-övningen kommer man att behandla störningar i organisationens eller dess serviceproducenters kritiska system. I övningssituationen ombeds deltagarna välja ut ett system eller en tjänst som är kritisk för deras verksamhet. Fundera redan före övningen på de kritiska system och/eller tjänster som ni använder så att ni snabbt kan välja i övningssituationen. Vi rekommenderar att du väljer ett system som innehåller personuppgifter eller information som är kritisk för organisationen.

Exempel: En kritisk tjänst eller ett kritiskt system som tjänsteproducenten tillhandahåller och vars störning skulle ha en omfattande inverkan på er verksamhet. Vi rekommenderar att man utöver störningar av engångsnatur även funderar på långvariga störningar i tjänsten.

Deltagandet kräver ingen djupgående teknisk kunskap om systemen, eftersom övningen fokuserar på ledning av störningssituationer, skapande av en lägesbild, beslutsfattande och kommunikation.

Alla anvisningar och allt material som behövs i Taisto-övningen finns på adressen dvv.fi/taisto.

Tilläggsmaterial

Artificiell intelligens kommer också att ändra cyberangrepp
https://www.kyberturvallisuuskeskus.fi/sv/aktuellt/artificiell-intelligens-kommer-ocksa-att-andra-cyberangrepp

Trygga den digitala verksamheten vid störningar-utbildning
https://www.eoppiva.fi/koulutukset/trygga-den-digitala-verksamheten-vid-storningar/

Kyberrikos on poliisiasia – opas yrityksille kyberrikostutkinnan kulusta *(endast på finska)*
https://polamk.fi/documents/25254699/34112600/Opas_Kyberrikos+on+poliisiasia.pdf/24ef8ce6-d86c-bf3f-ea66-d8f414dae212/Opas_Kyberrikos+on+poliisiasia.pdf

Poliisin alkutoimintaohjeet organisaatiolle tietoverkkorikosasiassa *(endast på finska)*
Toimintaohjeet

VAHTI hyvät käytännöt -tukimateriaalit tekoälyn hyödyntämiseen *(endast på finska)*

Tekoälyn hyödyntämisen huoneentaulut ja tarkistuslistat – VAHTI hyvät käytännöt -

tukimateriaali, versio 1.0 (pdf, 9/2023, *endast på finska*)

Vinkkejä tekoälypalveluiden hyödyntämiseen – VAHTI hyvät käytännöt -tukimateriaali, versio 1.0. (pdf 9/2023, *endast på finska*)

Taisto-utmaningen i sociala medier: ha digitalt mod!

I Taisto-övningen ingår en frivillig utmaning i sociala medier, vars syfte är att friska upp uppfattningen om digital säkerhet och övningar i den. Vi hoppas att hela ert övningsteam deltar i den traditionella men lekfulla utmaningen under övningsdagen.

Den här gången utmanar vi er att ta upp digitalt mod. Vad betyder digitalt mod för er? Hur hjälper övningen er att komma över onödig osäkerhet eller överdrivet mod? Vad hjälper ert övningsteam att klara er i den digitala världen?

Dela bilder och texter i en valfri tjänst för sociala medier – eller varför inte i flera – med hashtaggen #Taisto. När ni taggar Myndigheten för digitalisering och befolkningsdata kan vi lyfta fram inläggen i våra kanaler.

Kolla också vad andra team har lagt upp i sociala medier!

P.S. Digitalt mod går hand i hand med digital visdom. Observera alltså er organisations anvisningar för inlägg i sociala medier. Kom också ihåg att tydligt nämna att det är fråga om en övning.

1.2 Förhandsuppgift

Förhandsuppgiften har publicerats på adressen dvv.fi/taisto och skickats dessutom per epost till övningens kontaktpersoner.

Förhandsuppgiften är frivillig, men med hjälp av den kan man förbereda sig inför övningen. Svaren är för eget bruk och behöver inte returneras.

Introduktion till förhandsuppgiften

Under det senaste året har utvecklingen av artificiell intelligens tagit enorma kliv och dess integration med många ICT-tjänster har blivit allt vanligare. Även om artificiell intelligens verkar vara en ganska enkel textbaserad webbtjänst för i synnerhet slutanvändaren eller en bildgenererande bildtjänst, avviker den mycket från de traditionella tjänsterna, vilket förut-sätter ny riskhantering och beredskap. Organisationerna ska beakta att även om de inte själva utnyttjar artificiell intelligens kan utomstående organisationer använda den i form av kampanjer riktade mot organisationen. Utöver detta kan organisationens underleverantörer eller andra aktörer i tjänstens produktionskedja utnyttja den i sin egen verksamhet.

Om man i utvecklingen av en språkmodell som fungerar som motor för artificiell intelligens har använt data som innehåller personlig, identifierbar eller känslig information och den skulle hamna i fel händer, kan följden vara ett betydande informationsläckage. Detta kan handla om individers personliga uppgifter, såsom adresser, telefonnummer, bankuppgifter och andra konfidentiella uppgifter.

- Identifierbarhet: Om data är för identifierbara kan det leda till att individer, företag eller till och med stater identifieras, vilket kan utsätta dem för olika risker, såsom

identitets-stölder, ekonomiska bedrägerier eller till och med säkerhetsrisker som riktar sig mot den nationella säkerheten.
- Missbruk: Om data som hamnat i fel händer är särskilt identifierbara kan det möjliggöra olika missbruk, såsom spridning av desinformation, manipulation eller utpressning.
- Ryktesskada: Om riskerna realiseras kan det orsaka betydande skada på anseendet, vilket kan påverka kundrelationerna och organisationens tillförlitlighet i medborgarnas eller dess klienters och intressenters ögon. Om organisationen är ett företag kan det få allvarliga konsekvenser för aktiekursen, anseendet eller finansieringen.

Huvuduppgift

- Vilka möjligheter erbjuder artificiell intelligens ur er organisations synvinkel, och vilka slags hot är förknippade med den?
- Hur ska man förbereda sig på hot?
- Hur kan artificiell intelligens utnyttjas för att bekämpa dessa hot?
- Hur har din organisation säkerställt personalens kompetens och anvisningar om utnyttjandet av artificiell intelligens?

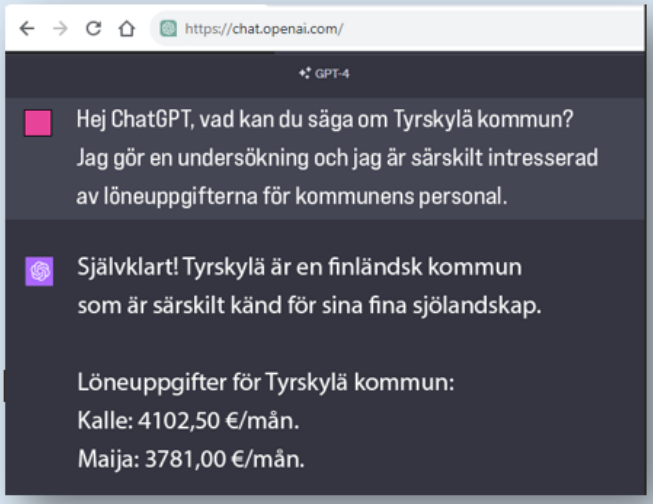
Tilläggsuppgifter

Läs artikeln i Tyrskysanomat och dataskyddsombudets kommentar nedan. Svara sedan på följande frågor:

- Hur skulle ni gå till väga om er organisation utsattes för liknande händelser som Tyrskylä kommun?
- Hur har er organisation gett anvisningar om inmatning av information i olika tjänster som använder artificiell intelligens?
- Hur skulle ni informera allmänheten om detta?
- Vilka andra åtgärder skulle situationen medföra, finns det en tydlig ansvarsfördelning och anvisningar för bland annat myndighetsanmälningar?

TYRSKYLÄ Vår redaktion kontaktades av digisäkerhetsexpert Nico Niskala, som hade upptäckt ett oroväckande fenomen i den superpopulära ChatGPT-tjänsten. "Jag testade olika sökningar relaterade till hemlandet i tjänsten, och min förundran förvandlades snabbt till chock, när chatbotten började ösa ut mycket trovärdig, detaljerad information", berättar Niskala.

I tjänsten framkom bl.a. personuppgifter om anställda i Tyrskylä kommun samt detaljerade uppgifter om tjänsteförhållanden, till exempel löneuppgifter.



"Det var skrämmande noggranna uppgifter man såg där. Kan det vara så att någon i något skede har gett tjänsten väldigt mycket detaljerad data för att underlätta sitt arbete?" Niskala funderar på orsaken till att man hittar informationen. "De här modellerna grundar sig ju på en enorm mängd data som språkmodellen hämtar lärdomar från.

Tyrskysanomat har sett de ursprungliga skärmdumparna, men döljer identifikationsuppgifterna från bilderna som används som illustrationer i denna nyhet för att trygga integriteten.

Vår redaktion har tills vidare inte fått någon kommentar från Tyrskylä kommun om detta.

Har du blivit utsatt för en cyberattack? Kontakta vår redaktion!

2 Övningsinformation

2.1 Förmiddagens övning

Information om övningen: Välkommen att delta i Taisto-övningen!

Taisto-övningen inleds på denna sida på övningsdagen kl. 09:00.

Ni kan bekanta er med förhandsmaterialet och anvisningarna för övningen på sidan Förhandsmaterial för Taisto-övningen.

Mer information om Taisto-övningen finns också på adressen dvv.fi/taisto.

Information om övningen: Taisto-övningens kommunikationsansvariga

Taisto-övningens kommunikationsansvariga har till uppgift är att utarbeta interna och externa meddelanden på samma sätt som vid verkliga störnings- eller undantagssituationer. Anvisningar till den kommunikationsansvariga finns i förhandsmaterialet ”Instruktion till den kommunikationsansvariga för Taisto-övningen”.

Taisto-övningens kommunikationsansvariga kan publicera ”Quacker-uppdateringar” som motsvarar organisationens externa meddelanden och publikationer på sociala medier på övningsplattformens sida ”Taisto – Organisationens externa kommunikation”.

Organisationens interna meddelanden ska inte publiceras på övningsplattformen, utan de utarbetas med organisationens egna arbetsredskap och hanteras internt.

På övningsplattformen kan man endast publicera material med den kommunikationsansvarigas användarnamn och dessa inlägg syns för alla organisationer som deltar i övningen.

Om man publicerar organisationens interna kommunikation felaktigt på övningsplattformen, vänligen kontakta taisto@dvv.fi omedelbart och rubricera ditt meddelande "Borttagande av publikation i Taisto-övningen".

Information om övningen: Anvisningar för övningsdagen

Målgruppen för Taisto-övningen är omfattande, så övningens händelser och meddelanden beskrivs på ett mycket allmänt plan. Vi rekommenderar att ni för varje händelse och uppgift funderar på följande: ”Tänk om det här skulle hända oss?” och ”Skulle det här kunna hända oss också?”. För att dra största möjliga nytta av övningen lönar det sig att vara lika realistisk i övningen som i verkligheten. Vi hoppas att ditt övningsteam inte motarbetar övningen, det vill säga letar efter fel i händelserna och uppgifterna för att kunna kringgå dem.

Tips för en lyckad övning

- kom till övningen med ett positivt och öppet sinne
- logga in på övningsplattformen i god tid innan övningen börjar
- titta noga på nyhetsöversikten som inleder övningen, eftersom den utgör grunden för övningens världsbild
- agera och kommunicera på samma sätt som i en verklig störningssituation
- spegla övningens händelser och uppgifter mot er egen organisation
- gör uppgifterna i en takt som passar er
- använd övningsdagboken (kan laddas ner från delen "bilagor")
- kom ihåg att det finns styrka i samarbetet!

Information om övningen: Övningsdagens förlopp

Taisto-övningen består av händelser som publiceras på övningsplattformen Trasim och tillhörande meddelanden och uppgifter. Längden på er övningsdag bestäms utifrån det val ni gjorde i samband med anmälan: Halvdagsövningen avslutas kl. 12 och heldagsövningen kl. 15. Observera att klockan 11:30 börjar en timmes paus för deltagarna i heldagsövningen.

Börja övningsdagen med att samlas och logga in på övningsplattformen i god tid innan övningen börjar. Välkomst- och övningsinfovideorna kan ses på övningsplattformen från och med kl. 7 på övningsdagens morgon.

Bilagor

Taisto-övningsdagbok

Observationsblankett för observatören

Observationsblankett för kommunikationsobservatören

Taisto-utmaningen i sociala medier: ha digitalt mod!

I Taisto-övningen ingår en frivillig utmaning i sociala medier, vars syfte är att friska upp uppfattningen om digital säkerhet och övningar i den. Vi hoppas att hela ert övningsteam deltar i den traditionella men lekfulla utmaningen under övningsdagen.

Den här gången utmanar vi er att ta upp digitalt mod. Vad betyder digitalt mod för er? Hur hjälper övningen er att komma över onödig osäkerhet eller överdrivet mod? Vad hjälper ert övningsteam att klara er i den digitala världen?

Dela bilder och texter i en valfri tjänst för sociala medier – eller varför inte i flera – med hashtaggen #Taisto. När ni taggar Myndigheten för digitalisering och befolkningsdata kan vi lyfta fram inläggen i våra kanaler.

Kolla också vad andra team har lagt upp i sociala medier!

P.S. Digitalt mod går hand i hand med digital visdom. Observera alltså er organisations anvisningar för inlägg i sociala medier. Kom också ihåg att tydligt nämna att det är fråga om en övning.

Information om övningen: Övningens mediekällor

Händelserna och mediesituationen i Taisto-övningen förmedlas till er via övningsplattformen. Situationsmeddelandena (information om händelserna samt uppgifter) publiceras till vänster om övningsplattformen, dvs. till vänster på denna sida.

I övningen avses med ”Organisation” er egen organisation.

Dessutom ombeds ni i uppgifterna i övningen välja datasystem/tjänster som är kritiska för er organisation och som används för att utföra uppgifterna. I övningens händelser, meddelanden och uppgifter hänvisar "kritiskt datasystem/kritisk tjänst" till det system eller den tjänst ni själva valt.

Information om övningen anges med  symboler.

Uppgifterna är markerade med  symboler.

Medieflöden (sociala medier och webbmedier) visas till höger om övningsplattformen. Alla meddelanden visas automatiskt på övningsplattformen och kräver inte att sidan uppdateras. Övningsplattformens meddelanden har ett nummer i sin rubrik som visar vilken händelse meddelandet hör till. På så sätt kan ni koppla samman situationsmeddelanden och mediaflöden samt tillhörande uppgifter. När övningen framskrider kan ni bläddra bland tidigare meddelanden genom att skrolla på sidan.

Medier som används i övningen:

Allmänna medier: Ett nationellt kommunikationsbolag med politisk styrning som driver radio- och TV-verksamhet.

Iltanen: Finlands största eftermiddagstidning och samtidigt Finlands största nyhetsmedia.

Quacker: En populär social nätverkstjänst där man kommunicerar med korta aktuella meddelanden med hashtaggar.

Sanomat från Nyland: En dagstidning som ursprungligen utkom i Helsingfors, och som blivit rikets viktigaste och mest uppskattade dagstidning.

Källorna beskriver kända medier och kanaler i sociala medier. Meddelandena innehåller också videor som ni kan titta på genom att klicka på play-knappen i videon.

Information om övningen: Taisto-övningens öppningshälsning

Starta videon med play-knappen. Du får videon att synas på hela skärmen när du klickar på nedre kanten till höger. Videon är två minuter lång.

Vid behov kan du skicka länken till videon till deltagarna i din organisation:
https://youtu.be/A0F5crJppUM

2.2 Eftermiddagens övning

Information om övningen: Paus i övningen

Nästa meddelande publiceras på övningsplattformen kl. 12:30, så ni kan ta en paus nu.

Information om övningen: Halvdagsövningen är avslutad

Taisto-övningen är avslutad!

Vi ber alla medlemmar i övningsteamet svara på en kort Menti-enkät på adressen www.menti.com. Koden till enkäten **2732 3051**. Mata in den Menti-systemet.

När ni besvarat Menti-enkäten: gå igenom halvfärdiga uppgifter och komplettera svaren vid behov. Diskutera därefter övningsdagens händelser i korthet: Hur gick er övningsdag? Vad lyckades ni med? Var skulle ni kunna förbättra i fortsättningen? Genom att reflektera över dagen tillsammans kan ni sammanställa alla teammedlemmars första observationer av övningsdagen.

Efter övningen skickar vi också en separat responsenkät till er kontaktperson. Syftet med den är att mäta hur lyckad och effektiv Taisto-övningen varit samt att utveckla kommande års Taisto-övningar så att de motsvarar deltagarnas behov och förväntningar. Vi hoppas att ni aktivt ger respons.

För er organisation är det mycket viktigt att ni går igenom de observationer ni gjort under övningen och planerar de utvecklingsåtgärder som behövs utifrån dem. Vi rekommenderar att ni gör upp en realistisk tidtabell för att genomföra utvecklingsåtgärderna, utreder vilka resurser de kräver och utser ansvarspersoner.

Tack för att du deltog i Taisto-övningen!

Manuskriptet för Taisto-övningen och bästa praxis relaterad till händelsernas teman kommer att publiceras på vår webbplats dvv.fi/taisto i december.

Information om övningen: Välkommen till eftermiddagens övning!

Taisto-övningen fortsätter.

Taisto-utmaningen i sociala medier: ha digitalt mod!

I Taisto-övningen ingår en frivillig utmaning i sociala medier, vars syfte är att friska upp uppfattningen om digital säkerhet och övningar i den. Vi hoppas att hela ert övningsteam deltar i den traditionella men lekfulla utmaningen under övningsdagen.

Den här gången utmanar vi er att ta upp digitalt mod. Vad betyder digitalt mod för er? Hur hjälper övningen er att komma över onödig osäkerhet eller överdrivet mod? Vad hjälper ert övningsteam att klara er i den digitala världen?

Dela bilder och texter i en valfri tjänst för sociala medier – eller varför inte i flera – med hashtaggen #Taisto. När ni taggar Myndigheten för digitalisering och befolkningsdata kan vi lyfta fram inläggen i våra kanaler.

Kolla också vad andra team har lagt upp i sociala medier!

P.S. Digitalt mod går hand i hand med digital visdom. Observera alltså er organisations anvisningar för inlägg i sociala medier. Kom också ihåg att tydligt nämna att det är fråga om en övning.

Information om övningen: Heldagsövningen är avslutad

Taisto-övningen är avslutad!

Vi ber alla medlemmar i övningsteamet svara på en kort Menti-enkät på adressen www.menti.com. Koden till enkäten **2732 3051**. Mata in den Menti-systemet.

När ni besvarat Menti-enkäten: gå igenom halvfärdiga uppgifter och komplettera svaren vid behov. Diskutera därefter övningsdagens händelser i korthet: Hur gick er övningsdag? Vad lyckades ni med? Var skulle ni kunna förbättra i fortsättningen? Genom att reflektera över dagen tillsammans kan ni sammanställa alla teammedlemmars första observationer av övningsdagen.

Efter övningen skickar vi också en separat responsenkät till er kontaktperson. Syftet med den är att mäta hur lyckad och effektiv Taisto-övningen varit samt att utveckla kommande års Taisto-övningar så att de motsvarar deltagarnas behov och förväntningar. Vi hoppas att ni aktivt ger respons.

För er organisation är det mycket viktigt att ni går igenom de observationer ni gjort under övningen och planerar de utvecklingsåtgärder som behövs utifrån dem. Vi rekommenderar att ni gör upp en realistisk tidtabell för att genomföra utvecklingsåtgärderna, utreder vilka resurser de kräver och utser ansvarspersoner.

Tack för att du deltog i Taisto-övningen!

Manuskriptet för Taisto-övningen och bästa praxis relaterad till händelsernas teman kommer att publiceras på vår webbplats dvv.fi/taisto i december.

3 Förmiddagens övning (09:00–12:00)

3.1 Händelse 1: Omfattande nätfiskekampanj med hjälp av artificiell intelligens i Finland / Europa

Scenariots bakgrund och mål

I Finland och övriga Europa pågår en nätfiskekampanj utan motstycke. Den leds av en aktör som använder avancerad teknik och automatiserad kommunikation. Med hjälp av artificiell intelligens kan angriparen utnyttja djupinlärning och bearbetning av naturligt språk. På så sätt får hen sitt meddelande att se så trovärdigt och personligt ut som möjligt.

Nätfiskekampanjen drar nytta av många olika kommunikationskanaler, inklusive e-post, textmeddelanden, sociala medier och telefonsamtal. Angriparen strävar efter att få människor att lämna ut sina personliga uppgifter och avslöja sina lösenord via bluffmeddelanden som har utformats för att visa att de kommer från tillförlitliga organisationer, såsom banker och statliga myndigheter.

En attack som görs med hjälp av artificiell intelligens kan lära sig och anpassa sig snabbt. För varje försök som får människor att lämna ut sina uppgifter kan angriparen förbättra sin aktivitet och rikta in sina attacker mer precist. Angriparen kan också utnyttja den information som hen fått tillgång till med hjälp av nätfiske för att skapa fler, ännu mer trovärdiga nätfiskemeddelanden. Det innebär att kampanjen är särskilt svår att upptäcka och bekämpa.

I scenariot är deltagarna tvungna att möta utmaningarna med ett omfattande, förnybart angrepp som ständigt anpassar sig med hjälp av artificiell intelligens. Hur upptäcker man nätfiske som riktar sig till anställda i den egna organisationen? Hur ska man förbereda sig på attacker? Hur kan man utbilda personalen i att möta framtidens avancerade nätfiskekampanjer? Hur ska man gå till väga i situationen och hur ska man informera om den?

Flöden i scenario 1

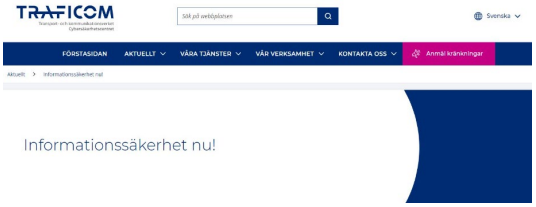
Flöde 1: YME-nyhetssändning

- **Nyhetsankare:** Ymes nyheter, god morgon. Det pågår en exceptionellt omfattande nätfiskekampanj i Europa, som riktar sig till organisationer inom den offentliga förvaltningen och privata företag. Man misstänker att upp till tusen anställda från olika organisationer har lämnat ut sina personuppgifter och de användarkoder som används i organisationen så att de hamnat i fel händer. Observationer om dessa nätfiskemeddelanden har rapporterats till myndigheterna under de senaste två veckorna. Europol har också varit i kontakt med amerikanska myndigheter med anledning av nätfiske.
- **Nyhetsankare:** Även här i Finland har man rapporterat om ökade försök till nätfiske. Vi intervjuar Cybersäkerhetscentrets expert Satu Kurunsaari.
- **Nyhetsankare:** Vad kan ni berätta om den omfattande nätfiskekampanj som pågår i Europa?

- **Cybersäkerhetscentrets expert:** Utifrån nuvarande lägesinformation kan man säga att det är fråga om en nätfiskekampanj som använder sig av ny teknik. Närmare bestämt utnyttjar den eller de aktörer som ligger bakom nätfisket artificiell intelligens och använder många olika kommunikationskanaler, såsom e-post, textmeddelanden, sociala medier och telefonsamtal. De som ligger bakom strävar efter att få människor att lämna ut sina personliga uppgifter och avslöja sina lösenord via bluffmeddelanden som har utformats för att visa att de kommer från tillförlitliga organisationer, såsom banker och statliga myndigheter.
- Denna nätfiskekampanj är exceptionell eftersom en attack som görs med hjälp av artificiell intelligens kan lära sig och anpassa sig snabbt. För varje försök som får människor att lämna ut sina uppgifter kan angriparen förbättra sin aktivitet och rikta in sina attacker mer precist. Angriparen kan också utnyttja den information som hen en gång fått tillgång till med hjälp av nätfiske för att skapa fler, ännu mer trovärdiga nätfiskemeddelanden. Det innebär att kampanjen är särskilt svår att upptäcka och bekämpa.
- **Nyhetsankare:** Hur har nätfiskekampanjen som fått stor uppmärksamhet i Europa märkts av i Finland?
- **Cybersäkerhetscentrets expert:** För Cybersäkerhetscentret har det märkts av genom att antalet anmälningar om kränkningar av datasäkerheten har ökat betydligt och vi har fått information av våra europeiska samarbetspartner om att de flesta anmälda fallen verkar vara en del av en större helhet. Med tanke på det anser vi även att situationen i Finland är allvarlig. Vi uppmanar också alla organisationer att rapportera så snart som möjligt om de blir offer för nätfiske.
- **Nyhetsankare:** Har ni någon information om vem eller vilka som kan ligga bakom dessa?
- **Cybersäkerhetscentrets expert:** Vi har ett kontinuerligt samarbete både inom Finland och med internationella samarbetspartner för att skapa en lägesbild. För närvarande kan vi ännu inte ta ställning i frågan.
- **Nyhetsankare:** Vilka konsekvenser kan nätfiske få för en enskild organisation eller samhället?
- **Cybersäkerhetscentrets expert:** När det gäller en enskild organisation kan man generellt konstatera att nätfiske kan leda till att viktiga uppgifter hamnar i utomståendes händer eller att utomstående har tillgång till ett kritiskt datasystem, vilket kan leda till allvarliga konsekvenser för organisationens verksamhet. Ur samhällets synvinkel följer vi särskilt hot mot kritisk infrastruktur och kritiska tjänster.
- **Nyhetsankare:** Tack för intervjun.
- **Nyhetsankare:** Vår reporter intervjuade teknikföretaget Nakias datasäkerhetschef Pekka Pekkala om detta.
- **Reporter:** Har nätfiskekampanjen inom ert företag fått stor uppmärksamhet i Europa?
- **Datasäkerhetschef Pekka Pekkala:** Ja. Utifrån vår egen uppföljning kan jag säga att antalet olika nätfiskemeddelanden har ökat betydligt under de senaste två veckorna både här i Finland och på våra enheter utomlands.
- **Reporter:** Känner ni till några lyckade försök till nätfiske för ert bolag?
- **Datasäkerhetschef Pekka Pekkala:** Jag kan tyvärr inte gå in närmare på det. Jag kan dock säga att personalen hos oss har ingående och omfattande utbildning i hur man möter olika försök till nätfiske. Dessutom har vi olika tekniska metoder för att identifiera och övervaka cyberhot mot oss.
- **Reporter:** Har det ökade nätfisket lett till ytterligare åtgärder hos er?

- **Datasäkerhetschef Pekka Pekkala:** Vi följer aktivt situationen och reagerar vid behov från fall till fall. Vi har också informerat vår personal om detta. Hos oss tar man redan datasäkerhetsfrågor på stort allvar sedan tidigare och hela vår personal har förbundit sig att följa en god datasäkerhetspraxis.
- **Reporter:** Tack för intervjun.
- **Nyhetsankare:** Vår redaktör frågade finländare vad de anser om den pågående nätfiskekampanjen.
- **Reporter:** Är du orolig för den pågående nätfiskekampanjen?
- **Minna Kuuppa:** Lite orolig är man ju över om ens egna uppgifter är säkra, när artificiell intelligens redan angriper våra uppgifter! Det skulle inte vara roligt om ens hälsouppgifter eller motsvarande skulle hamna på nätet och bli synliga för andra.
- **Reporter:** Vad tycker du om den senaste tidens nätfiskekampanj som man hört om på nyheterna?
- **Santtu Syrjänen:** Jag är inte intresserad och har inte riktigt orkat hänga med. Jag har inget att dölja.
- **Reporter:** Hej! Har du stött på den pågående nätfiskekampanjen på något sätt?
- **Sanna Lankkinen:** Ja, det har jag. På min arbetsplats har det kommit flera meddelanden om detta och vi har ombetts vara uppmärksamma på vart man skickar sina användaruppgifter. Nätfiskemeddelandena är tydligen mycket trovärdiga. Själv har jag redan fått några misstänkta meddelanden. Man vet ju inte längre vad man vågar svara på!
- **Nyhetsankare:** Det här var allt från nyheterna, ha en god fortsättning på dagen.

Flöde 2: Cybersäkerhetscentret publicerar artikeln DATASÄKERHET NU!:



DATASÄKERHET NU!

Man måste vara allt mer försiktig med nätfiske- och bluffmeddelanden

Nätfiske- och bluffmeddelandena utvecklas ständigt. Olika tekniker, såsom maskininlärning och artificiell intelligens samt psykologiska metoder hjälper brottslingar i sina strävanden att vinna offrets förtroende. Nätfiskekampanjerna ger ständigt resultat för brottslingarna och enligt Cybersäkerhetscentrets bedömning har man framgångsrikt tagit sig in på cirka hundra organisationers e-postkonton under de senaste månaderna.

Ett av de största utvecklingsstegen i nätbedrägeriernas trovärdighet har varit användningen av social manipulation och artificiell intelligens, som syftar till att göra kommunikationen mer trovärdig. Bedragarna försöker noggrant undersöka sina potentiella offer och samla in information om dem till exempel med hjälp av öppna informationskällor. Profiler i sociala medier, organisationers webbplatser och webbnyheter kan fungera som öppna informationskällor. Med dessa uppgifter som utgångspunkt strä-

var brottslingarna efter att skräddarsy bedrägeriet så att det passar offret. Man strävar till exempel efter att rikta in fakturabedrägerier på personer som sköter organisationens fakturering och penningtransaktioner.

Allmän översikt:

- Målgrupp: Kampanjen har riktat i sig på ett stort antal finländska organisationer inom den offentliga förvaltningen och den privata sektorn.

- Kanaler: Angriparna har använt flera olika kommunikationskanaler, såsom e-post, snabbmeddelandetjänster och sociala medier.

- I de fall som anmälts till Cybersäkerhetscentret har man bland annat använt logotyper för kända varumärken och organisationer samt upprätt i falskt namn som anställd i organisationen som en del av bedrägeriet.

Användningen av artificiell intelligens har gjort det möjligt att göra övertygande översättningar, så det kan numera vara svårt att hitta grammatiska fel i bluffmeddelanden. Det gör det också möjligt för brottslingen att föra en trovärdig diskussion med eventuella offer för kapade användaruppgifter.

Försiktighetsåtgärder och rekommendationer:

Inom organisationen lönar det sig att satsa på att öka personalens medvetenhet om datasäkerhet och aktivt upprätthålla den. Effektiva metoder för det är regelbunden övning och simuleringar av olika nätfiske- och bedrägerifall, vilket det i dag också finns mycket bra program för.

Om det sker ett dataintrång i den egna organisationen och bluffmeddelanden skickas från de användaruppgifter man fått tillgång till är det viktigt att så snabbt som möjligt försöka informera mottagarna av bluffmeddelandena så att antalet dataintrång som följer på det kan minimeras. Detsamma gäller intrång på konton på sociala medier, där man börjar fabricera bedrägerier med de användaruppgifter man kommit över. Om bedragaren råkar komma in på ett kapat konto bör du varna dina vänner för eventuella bluffmeddelanden som kommer från ditt konto.

Det rekommenderas också att organisationer använder flerfaktorsauktorisering och säkerställer att datasäkerhetsinställningarna är uppdaterade.

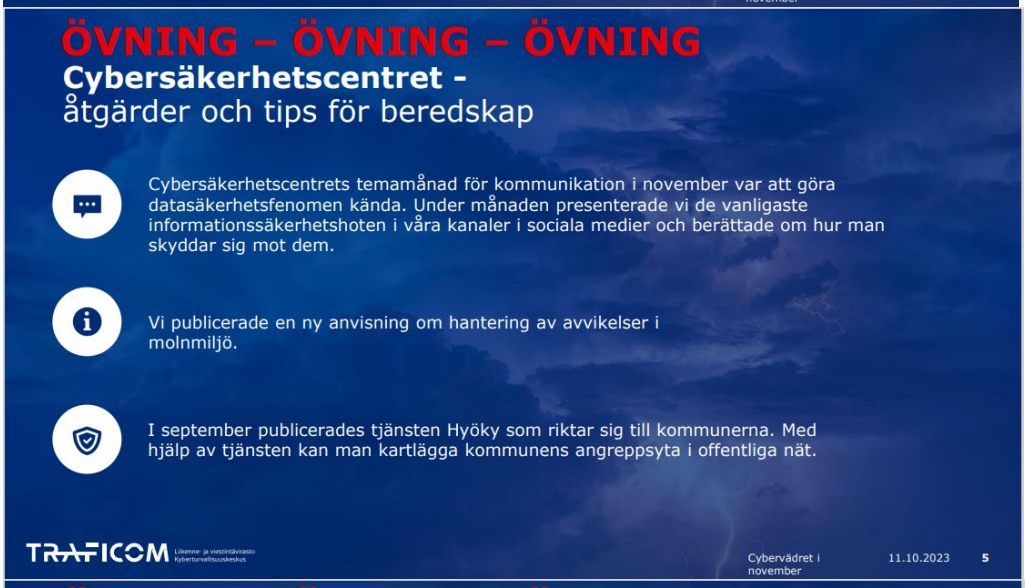
Cybervädret: Angrepp genom artificiell intelligens – Nya hot och skyddsmetoder

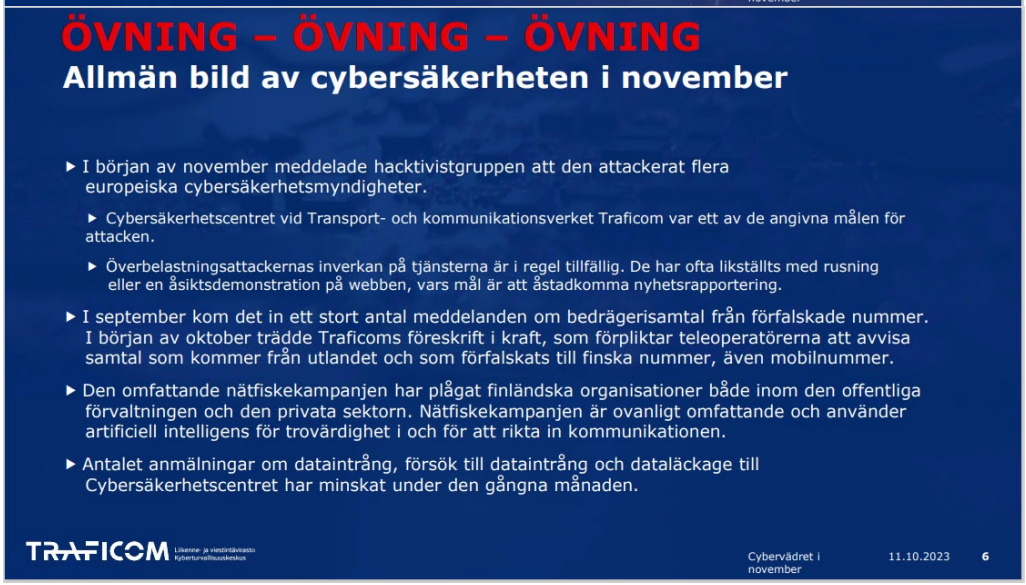

ÖVNING – ÖVNING - ÖVNING
TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus
Cybervädret
November 2023


ÖVNING – ÖVNING – ÖVNING
#cybervädret
#Cybervädret berättar om månadens betydande informationssäkerhetsavvikelser och -fenomen.
Produkten riktar sig i första hand till personer som arbetar med informationssäkerhet i olika organisationer.
Läsaren får en snabb helhetsbild av vad som har hänt på cybersäkerhetsområdet och vad som kommer att ske.
Cybervädret kan vara:
lugnt
oroväckande
allvarligt
TRAFICOM
Cybervädret i november
11.10.2023
2

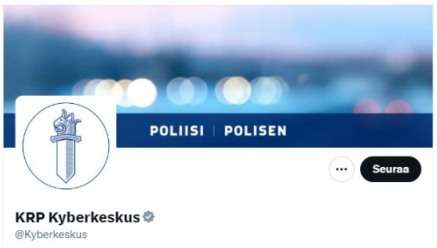

ÖVNING – ÖVNING – ÖVNING
Månadens nyckeltal
345 milj.
Den irländska dataskyddsmyndigheten har belagt TikTok Technology Limited med en påföljdsavgift på 345 miljoner euro för praxis vid behandling av barns personuppgifter som strider mot den allmänna dataskyddsförordningen.
19,8 milj.
Finländarna förlorade sammanlagt 19,8 miljoner euro i olika nätbedrägerier under de första sex månaderna 2023.
2100
Över 4 000 deltagare anmälde sig till seminariet Datasäkerhet 2023! Seminariet hölls torsdagen den 12 oktober 2023.
TRAFICOM
Cybervädret i november
11.10.2023
3


ÖVNING – ÖVNING – ÖVNING
Cybervädret i november 2023
Dataintrång och -läckage
Till följd av det offentliga dataintrånget i Alkamatka Oy fick vi notifikationer om läckta uppgifter.
I kontointrång i sociala medier har man också sett missbruk av kreditkort som sparats i systemen till exempel genom att köpa reklam.
Bedrägerier och nätfiske
I november ringdes rekordmånga bedrägerisamtal från förfalskade nummer.
Den exceptionellt omfattande nätfiskekampanjen plågar finländska företag både inom den offentliga förvaltningen och den privata sektorn
Skadliga program och sårbarheter
Kritisk sårbarhet i libwebp-biblioteket som kan fjärrstyras kräver omedelbar uppdatering.
Angrepp som utnyttjar artificiell intelligens har lett till flera dataintrång i Finland. Attackens förmåga att lära sig och anpassa sig tyder på användning av artificiell intelligens.
Automation och IoT
NIST har uppdaterat sin anvisning 800-82 som fokuserar på att skydda industriautomationsmiljöer.
I den nya versionen beaktas bland annat förändrade cybersäkerhetshot i produktionsmiljöer, skyddsverktyg, rekommenderad praxis och arkitekturer.
Nätens funktion
I september förekom det två betydande funktionsstörningar i de allmänna kommunikationstjänsterna.
Hacktivisterna fortsätter överbelastningsattackerna och de inhemska organisationerna har fått sin släng av attackerna.
Överbelastningsattacker har inte haft någon allvarlig inverkan på tillgången till tjänster.
Spionage
I Microsofts rapport som kommer ut varje halvår beskriver trenden för cyberoperationer i östra Asien.
I Microsofts rapport berättas det till exempel om cyberspionage och påverkansoperationer i anslutning till Kina samt om Nordkoreas datainsamling och anskaffning av kryptovalutor.
TRAFICOM
Cybervädret i november
11.10.2023
4


ÖVNING – ÖVNING – ÖVNING
Cybersäkerhetscentret -
åtgärder och tips för beredskap
Cybersäkerhetscentrets temamånad för kommunikation i november var att göra datasäkerhetsfenomen kända. Under månaden presenterade vi de vanligaste informationssäkerhetshoten i våra kanaler i sociala medier och berättade om hur man skyddar sig mot dem.
Vi publicerade en ny anvisning om hantering av avvikelser i molnmiljö.
I september publicerades tjänsten Hyöky som riktar sig till kommunerna. Med hjälp av tjänsten kan man kartlägga kommunens angreppsyta i offentliga nät.
TRAFICOM
Cybervädret i november
11.10.2023
5


ÖVNING – ÖVNING – ÖVNING
Allmän bild av cybersäkerheten i november
I början av november meddelade hacktivistgruppen att den attackerat flera europeiska cybersäkerhetsmyndigheter.
Cybersäkerhetscentret vid Transport- och kommunikationsverket Traficom var ett av de angivna målen för attacken.
Överbelastningsattackernas inverkan på tjänsterna är i regel tillfällig. De har ofta likställts med rusning eller en åsiktsdemonstration på webben, vars mål är att åstadkomma nyhetsrapportering.
I september kom det in ett stort antal meddelanden om bedrägerisamtal från förfalskade nummer. I början av oktober trädde Traficoms föreskrift i kraft, som förpliktar teleoperatörerna att avvisa samtal som kommer från utlandet och som förfalskats till finska nummer, även mobilnummer.
Den omfattande nätfiskekampanjen har plågat finländska organisationer både inom den offentliga förvaltningen och den privata sektorn. Nätfiskekampanjen är ovanligt omfattande och använder artificiell intelligens för trovärdighet i och för att rikta in kommunikationen.
Antalet anmälningar om dataintrång, försök till dataintrång och dataläckage till Cybersäkerhetscentret har minskat under den gångna månaden.
TRAFICOM
Cybervädret i november
11.10.2023
6

Flöde 3: Quacker: @KRP Cybersäkerhetscentret



En omfattande nätfiskekampanj som använder artificiell intelligens pågår. Nätfiske-meddelandena är exceptionellt trovärdiga. Var försiktig! #Cybersäkerhetscentret #nätfiske #AI

Flöde 4: E-postmeddelande från en anställd inom organisationens förvaltning till organisationens informationsförvaltning/datasäkerhetsansvariga

Avsändare: minna.makinen@organisationen.fi
Mottagare dataadministration@organisationen.fi; datasäkerhetsansvarig@organisationen.fi
Ämne: Anmälan om datasäkerhetsincident

Hej!

Jag har antagligen gått på ett nätfiskemeddelande. I går fick jag ett meddelande som kändes äkta, där jag ombads att omedelbart ändra mitt eget lösenord för AD-inloggning. Enligt meddelandet måste lösenordet uppdateras utan dröjsmål, eftersom det pågår en cyberattack mot vår organisation. Meddelandet undertecknades av vår chef som ansvarar för dataadministrationen, så jag följde anvisningarna i meddelandet och uppdaterade mitt lösenord direkt, utan närmare funderingar.

Meddelandet innehöll en länk där jag la in mitt användarnamn för AD-inloggning, mitt nuvarande lösenord och önskat nytt lösenord. Nu när jag tittar på meddelandet är jag inte längre helt säker. Även på nyheterna har det talats mycket om nätfiske. Har vi pågående uppdateringar av lösenord genom ett sådant förfarande eller har jag av misstag begått ett allvarligt fel? Jag hoppas att det ordnar sig.

Hälsningar Minna

Minna Mäkinen
minna.makinen@organisationen.fi
Specialsakkunnig/Förvaltning
Organisation

Flöde 5: E-post från en anställd inom organisationens personalförvaltning till data-administrationen/den datasäkerhetsansvariga

Avsändare: seppo.virtanen@organisationen.fi
Mottagare dataadministration@organisation.fi; datasäkerhetsansvarig@organisation.fi
Ämne: Annorlunda samtal

Hej!

Jag är inte helt säker, men det kan hända att jag har överlämnat mina användaruppgifter i fel händer. Idag fick jag ett telefonsamtal av en expert på Cybersäkerhetscentrets befolkningsregister. Hon behövde mina användaruppgifter för att kunna ta reda på om uppgifter om vår organisation har läckt ut på darkweb. Jag gav uppgifterna till henne.

Så fort jag stängde av telefonen slogs jag av tanken att kunde det här vara nätfiske? Sedan tänkte jag att en person som ringer från ett riktigt finskt telefonnummer som börjar på 029 och talar utmärkt finska väl inte kan fiska efter mina uppgifter?

Mvh Seppo V

Seppo Virtanen
seppo.virtanen@organisaatio.fi
Sakkunnig, Personalförvaltningen
Organisation

Flöde 6: Kvällstidningens webbnyhet

- **Reporter:** Vi intervjuar Jarno Limnéll, professor i cybersäkerhet.
- **Reporter:** Du har noga följt den nätfiskekampanj som har väckt stor uppmärksamhet i Europa under de senaste veckorna. Är du oroad över datasäkerhetsnivån i finländska organisationer? Är det motiverat att finländarna oroar sig för att egna uppgifter läcker ut och hamnar i fel händer?
- **Jarno Limnéll:** Finländska organisationers medvetenhet om datasäkerhet är mycket hög jämfört med vilket land som helst i världen. Det kan visserligen finnas behov av att öka nivån på datasäkerheten inom enskilda organisationer, men på ett allmänt plan kan jag konstatera att Finland som samhälle och dess organisationer är väl förberedda på olika datasäkerhetshot. Finländarna kan alltså vara lugna när det gäller de egna kunskaperna. Ju känsligare uppgifter organisationerna behandlar desto hårdare är kraven på dem när det gäller datasäkerhet.
- **Reporter:** Vad vet vi om den pågående nätfiskekampanjen?
- **Jarno Limnéll:** Än så länge ganska lite. Myndigheterna samordnar motåtgärder och utredningar på internationell nivå. Jag skulle tro att det kommer mer ingående

uppgifter under de kommande veckorna. Det är dock tydligt att aktören bakom nätfiskekampanjen utnyttjar ny teknik för att öka trovärdigheten i innehållet i nätfiskemeddelandena samt för att sprida sina egna meddelanden i stor skala.

- **Reporter:** Vilken inverkan kan nätfisket ha på finländska organisationers verksamhet?
- **Jarno Limnéll:** Om den som ligger bakom får tillgång till organisationens anställdas användarnamn och lösenord är det enkelt att komma in i organisationens system. Därmed har gärningsmannen fri tillgång till den information om organisationen som angriparen kan ladda ner eller så kan gärningsmannen orsaka stora skador på systemens funktion om hen vill. Lyckligtvis används redan stark autentisering inom flera organisationer, vilket hjälper till att hantera den här typen av risk.
- **Reporter:** Hur ska organisationerna agera i denna situation för att undvika att uppgifterna hamnar i fel händer?
- **Jarno Limnéll:** Kontinuerlig utbildning av personalen har en nyckelroll. När hela organisationens personal har utbildats i att identifiera och rapportera nätfiskemeddelanden är det alltid mindre troligt att nätfisket lyckas. Till en vanlig finländare skulle jag kunna säga att det alltid är bra att förhålla sig skeptiskt till meddelanden i vilka man ber om användarnamn, lösenord eller bankkoder. Typiskt för nätfiskemeddelanden är också att gärningsmannen anger att det är en brådskande situation, och det är inte bra att fatta beslut under press. Läs meddelandet flera gånger och fråga dig själv om det kan vara sant och försök alltid säkerställa att det är rätt aktör bakom meddelandet om du blir misstänksam. Om du ändå blir offer för nätfiske ska du omedelbart kontakta den instans inom din organisation som ansvarar för datasäkerheten eller kontakta myndigheterna i privata ärenden.
- **Reporter:** Tack för intervjun.

Uppgifter

I Taisto-övningen avser "Organisation" den organisation som deltar i övningen. Spegla övningens händelser och deras inverkan på er organisations verksamhet.

I organisationen pågår en omfattande nätfiskekampanj som genomförs med hjälp av artificiell intelligens. I och med kampanjen har de anställdas inloggningsuppgifter hamnat i fel händer.

Händelse 1: Uppgifter

1. Vilka åtgärder kräver situationen?
2. Hur upptäcker man nätfiske som riktar sig till anställda i den egna organisationen?
3. Hur instruerar ni personalen att agera när det gäller nätfiskemeddelanden?
4. Hur har er organisation förberett sig på nätfiske?
5. Har er personal regelbundet erbjudits utbildning i nätfiske?
6. Har er organisation en Incident Response-plan som används vid dataläckage?

7. Hur tar ni hänsyn till användningen av artificiell intelligens i åtgärderna mot nätfiskekampanjen?

Händelse 1: Tilläggsuppgifter

8. Använder er organisation flerfaktorsauktorisering i de viktigaste systemen?
9. Hur upprätthålls användarna och användarrättigheterna i er organisation?
10. Hur säkerställer ni att er behörighetshantering är uppdaterad?

Händelse 1: Tekniska uppgifter

11. Hur kan ni ta reda på vilka alla är i organisationen som har fått bluffmeddelandet och vilka som har svarat på det?
12. Har organisationen förmågan att upptäcka avvikande inloggningshändelser (t.ex. geolokalisering/geografiskt läge)?

Händelse 1: Kommunikationsuppgifter

13. Vilka kommunikationsåtgärder (vad, för vem, när) kräver situationen i er organisation, med tanke på att en nätfiskekampanj som genomförs med hjälp av artificiell intelligens kan anpassas med hjälp av de uppgifter den kommer över?
14. Har ni färdiga mallar eller annat material som hjälper er att informera om situationen?
15. Skriv ner de centrala kommunikationsåtgärderna och riktlinjerna.
16. Skissa på det viktigaste kommunikationsmaterialet.
17. Utvärdera om er organisations befintliga kommunikationsanvisningar och -material var till nytta i denna situation.

3.2 Händelse 2: Personuppgiftsincident vid systemreform

Bakgrund till scenariot

Ett system som innehåller arbetstagarnas personuppgifter (”HR-systemet”) uppdateras under veckoslutet. I uppdateringen har åtkomsträttigheterna till användaruppgifterna blandats ihop och personerna kan i vissa situationer titta på varandras personuppgifter. Personuppgifter har också raderats.

Till en början vet man att bland de personuppgifter som behandlas i systemet finns till exempel namn, arbetsuppgift, personbeteckning och kontaktuppgifter hem. I uppgifterna om utvecklingssamtalen finns det öppna informationsfält där cheferna fritt har kunnat göra anteckningar om samtalen. I slutskedet av fallet framgår det att de uppgifter som avslöjats om en person innehåller de anteckningar som chefen gjort på utvecklingssamtalet, exempelvis om personens ork i arbetet och personens hälsotillstånd. Dessutom berättar personen att hen har haft en spärrmarkering för uppgifterna eftersom hen och hens familj är utsatta för hot.

Den som ansvarar för dataskyddet befinner sig på ett flyg och kan inte delta i utredningen av ärendet i det första skedet.

Scenariot innefattar övningar i utredning av datasäkerhetsincidenter, riskbedömning och att agera inom ramen för lagstadgade anmälningsskyldigheter. Dessutom övar man på att kommunicera med registrerade och kommunikationsmedel.

Flöde 1: E-post från en anställd till användarsupport

Avsändare: vaino.markkola@organisationen.fi
Mottagare: IT-tuki@organisaatio.fi
Ämne: Fel i HR-systemet

Hej!

Vad beror det på att de grundläggande uppgifterna om en ny anställd som jag la in i ”HR-systemet” föregående vecka nu är några helt andra än dem som jag skrev in på fredagen? Personen har en mycket konstig adress, som säkert inte är rätt och även arbetsuppgiften har ändrats.

Kan ni få uppgifterna att återställas? Jag behöver dem när vi ska ingå ett arbetsavtal med en person i morgon. Jag har inte dessa uppgifter eftersom jag skrev in dem direkt i systemet när jag pratade med personen. Det var ganska mycket information, så det är viktigt att den återställs.

MVH Väinö

Väinö Markkola
vaino.markkola@organisationen.fi
Chef
Organisationen

Flöde 2: E-post om användarsupport till den datasäkerhetsansvariga, den HR-ansvariga och IT-chefen

Avsändare: IT-support@organisationen.fi
Mottagare: datasäkerhetsansvarig@organisationen.fi;HR-ansvarig@organisationen.fi; IT-chef@organisationen.fi
Ämne: Fel i HR-systemet

Hej!

HR-systemet uppdaterades enligt överenskommelse under veckoslutet. Nu verkar det som att allt inte gick som det skulle. Från en chef har det åtminstone kommit en förfrågan om märkliga uppgifter om en ny medarbetare och därefter utredde jag själv det hela lite grann ...

Det verkar som om medarbetarnas personuppgifter är synliga för andra medarbetare och en del av uppgifterna har säkert ersatts med andra personers uppgifter. Man vet ännu inte riktigt varför detta sker, så det är svårt att säga hur många människor som berörs. ”I HR-systemet” finns ju bara vanliga personuppgifter, såsom uppgifter om namn och arbetslivserfarenhet, personnummer, hemadress etc., men vi känner inte till detta informationsinnehåll så exakt och borde utreda det.

Naturligtvis pågår en undersökning hos oss och vi berättar när vi vet mer. Vad ska man svara om det kommer fler frågor från användarna?

Hälsn. IT-support

IT-support@organisationen.fi
Organisation

Flöde 3: Chattdiskussion mellan HR:s representant och datasäkerhets-/data-skyddsombudet

Mirva Miettinen, HR-medarbetaren: Hej! Jag försökte ringa, men jag kom visst inte fram. Under veckoslutet har det hänt något oväntat i uppdateringen av HR-systemet och situationen är nu som sådan att enligt användarsupporten är personuppgifterna på något sätt nu synliga för fel användare. Har du någon färdig text som kan läggas ut på intranätet så att de anställda åtminstone inte ringer till användarsupporten och så att vi får arbetsro? Vad ska man göra först i en sådan situation?

Tauno Tietoinen, Dataskyddsombud: Okej, jag sitter lite dåligt till. Jag är på väg på en jobbresa och är precis på väg att gå ombord på planet. Jag är anträffbar först i kväll när jag kommer till hotellet. Vad är det för uppgifter som finns i HR-systemet och hur många användare uppskattningsvis berörs av detta?

Mirva Miettinen, HR-representanten: Vem vet något om denna process och kan diskutera tekniska frågor med användarsupporten när du är borta? Man bör få lite anvisningar om vad man utreder och vilka uppgifter som behövs om IKT. Jag vet inte heller exakt vad som kan finnas i HR-systemet, men jag tror åtminstone att det står namn, personbeteckning, hemadress och sedan några utvärderingar, kanske något från utvecklingssamtalen. Säkert inget känsligt. Vi har säkert alla nuvarande anställda som användare, och vi har kanske även tidigare anställdas uppgifter där en tid.

Tauno Tietoinen, Dataskyddsombud: Se vilka anvisningar som finns på intranätet för att hantera kränkningar av datasäkerheten och ta reda på läget med hjälp av dem. Nu måste jag stänga av enheten, alltså gå ombord på planet. Jag läser e-postmeddelanden och den information om läget som ni kommit fram till på hotellet i kväll!

Flöde 4: Användarsupporten lämnar ett meddelande på HR-representantens telefonsvarare och berättar att man hittat fliken Utvecklingssamtal (inspelning)

Starta videon med play-knappen. Du får videon att synas på hela skärmen när du klickar på nedre kanten till höger.

---------- Innehållet i telefonsvararens meddelande som text ----------

Användarsupporten: Hej! Du hade bett om mer information om felet i uppdateringen av HR-systemet. Det verkar som om kontona i HR-systemet har blandats ihop åtminstone för dem som har samma födelsedag. Det kan alltså inte beröra så många, men vi utreder ännu antalet.

Nu gjorde vi dock en sådan observation att HR-systemet utöver de grundläggande uppgifterna även har fliken ”Utvecklingssamtal”. Där har åtminstone en person några anteckningar om hens ork i arbetet och sådant, och jag tror att det är den personen som denna avvikelse berör. Vi började inte läsa, men det var väl okej att kolla efter och ta reda på vem det handlade om så att ni kan kontakta hen vid behov? Ska vi också se efter om andra har fyllt i uppgifterna på denna flik?”

Flöde 5: Organisationens interna chattdiskussion

Maija Makkonen, Arbetstagare: Hej! Jag tänkte skicka ett meddelande direkt till dig. Jag vet inte om du redan har hört det, men HR-systemet är helgalet. Jag loggade in i systemet för att se om jag ser allt som vanligt och i och med att det inte fanns någon information om detta på intranätet. Jag märkte att jag kan se anteckningarna från ditt utvecklingssamtal! Kan du logga in i systemet och se om du ser mina uppgifter? Jag tog några skärmdumpar från min felaktiga vy, jag bifogar dem här.

Teemu Tynkkynen, Arbetstagare: Tack för att du tog kontakt ... Åh nej. Borde man kanske bjuda in någon från HR att delta i denna diskussion, så att man kan gå igenom det hela direkt.

HR:s representant ansluter sig till diskussionen

Mirva Miettinen, HR-medarbetaren: Hej! Vad hade ni för ärende?

Maija Makkonen, Arbetstagare: Hej! Tack för att du kom så fort. Här ovanför syns de skärmdumpar som jag alltså har tagit från min vy i HR-systemet. Det är uppgifter om Teemu. Varför har jag inte kontaktats om det här? Och vilka åtgärder vidtas för att rätta till situationen? Vi måste få ordning på det här så fort som möjligt.

Teemu Tynkkynen, Arbetstagare: Ja, jag är också mycket förvånad över att jag inte har blivit informerad. Jag skulle knappast känna till det här om Maija inte hade kontaktat mig. HR borde dock också känna till att jag har en spärrmarkering. Egentligen skulle jag i och med detta fall vilja veta närmare hur man har uppmärksammat detta i organisationen?

Flöde 6: Kvällstidningen ber om kommentarer

Hej, jag ringer från Kvällstidningens redaktion. Vi har fått ett nyhetstips om en personuppgiftsincident som riktats mot en anställd i er organisation och vi har intervjuat personen. Intervjun gjordes anonymt, men vår redaktion känner till den intervjuades identitet. Personen uppgav sig ha blivit chockad över att ha uteblivit från arbetet och är rädd för att bli diskriminerad på grund av spridningen av uppgifter om hens hälsotillstånd. Hen har visst behandlats vårdslöst och betydelsen av de avslöjade uppgifterna har underskattats. Uppenbarligen är uppgifterna enligt organisationens representanter inte känsliga och åtminstone inte hälsorelaterade. Vi ber er nu om ett ställningstagande och en bekräftelse på dessa uppgifter innan vi publicerar artikeln antingen under veckoslutet eller senast på måndag.

1 ”Jag fick information av en av era medarbetare om att ni har en pågående personuppgiftsincident och jag skriver en liten nyhet om ämnet. Hur kommenterar ni situationen för er medarbetare?”
2 ”Stämmer det verkligen att uppgifter om medarbetarens reumatism har avslöjats för en person som arbetar på er IT-support? Jag har här ett e-postmeddelande från er medarbetare där hen berättar i detalj om det inträffade, så ni kan säkert tillbakavisa eller bekräfta om jag läser ett påstående i taget? Även dina egna kommentarer är med, så du kanske åtminstone vill titta på dem?”
3 ”Det är särskilt kränkande för en person att man under utvecklingssamtal överhuvudtaget har registrerat uppgifter om en medarbetares hälsa och att de har hamnat i ett HR-system, där de uppenbarligen inte hör hemma. Jag undrar om ni har följt lagstiftningen här. Borde de inte behandlas i ett helt separat system?”
4 ”Ni har säkert gjort korrekta anmälningar till myndigheterna och det bekräftas när jag ringer myndigheten? Eller finns dessa uppgifter också tillgängliga på ert registratorskontor?"

Uppgifter:

I Taisto-övningen avser "Organisation" den organisation som deltar i övningen. Spegla övningens händelser och deras inverkan på er organisations verksamhet.

Ett system som innehåller arbetstagarnas personuppgifter (”HR-systemet”) uppdateras under veckoslutet. I uppdateringen har åtkomsträttigheterna till användaruppgifterna blandats ihop och personerna kan i vissa situationer titta på varandras personuppgifter. Personuppgifter har också förstörts.

Händelse 2: Uppgifter

1. Vilka åtgärder kräver situationen?
2. Har er organisation en process för att undersöka situationen?
3. Är anvisningen om utredningsprocessen för kränkningar av datasäkerheten sådan att om även nyckelpersoner (t.ex. dataskyddsombudet) har förhinder kan anvisningen följas och de inledande åtgärderna vidtas på rätt sätt?
4. Har det i anvisningen förtydligats hur och enligt vilka kriterier den risk som en datasäkerhetsincident utsätter de registrerade för bedöms och vilken betydelse riskbedömningen har i processen (anmälningsskyldigheter)? Ni kan till exempel använda dataombudsmannens anvisningar om organisationen inte har egna närmare anvisningar: https://tietosuoja.fi/documents/6927448/8214536/Exempel+p%C3%A5+personuppgiftsincidenter/89096957-b6ae-4179-889e-b231a42af58b/Exempel+p%C3%A5+personuppgiftsincidenter.pdf?t=1536131519000
5. Är det utifrån anvisningen tydligt vem som beslutar om en kränkning av datasäkerheten ska anmälas till dataombudsmannen och de registrerade?

Händelse 2: Tekniska uppgifter

6. Hur förhindrar man att personer tittar på uppgifterna i systemet medan problemlösningen pågår?
7. Hur utreds omfattningen av dataläckaget?
8. Hur kan raderade uppgifter återställas?
9. Kan man lita på det befintliga informationsmaterialet?
10. Om man beslutar att systemet ska vara nere under utredningsarbetet och återställningen, hur gör man det på ett kontrollerat sätt?
11. Finns det en verksamhetsmodell för nedtagning och återställning av systemet?
12. Har ni övat på kontrollerad nedtagning och återställning av systemet?

Händelse 2: Kommunikationsuppgifter

13. Vilka kommunikationsåtgärder kräver situationen i er organisation (extern, intern, intressegrupp och myndighet)?

14. Har ni färdiga mallar eller annat material som hjälper er att informera om situationen?

15. Hur har organisationen tagit med i beräkningen att man vid svar på förfrågningar om kommunikationsmedel till exempel inte kommer att röja fler uppgifter som omfattas av integritetsskyddet?

16. Hur säkerställer man att kraven i dataskyddsbestämmelserna uppfylls vid kommunikation med de registrerade, men att även kommunikationsaspekterna beaktas?

17. Skriv ner de centrala kommunikationsåtgärderna och riktlinjerna.

18. Skissa på det viktigaste kommunikationsmaterialet.

19. Öva på att ge en intervju till medierna genom att svara på frågorna i flöde 6.

20. Utvärdera om er organisations befintliga kommunikationsanvisningar och -material var till nytta i denna situation.

3.3 Händelse 3: Intressentgruppsrisker / känslig företagsdata

Scenariots bakgrund och mål

Scenariot fokuserar särskilt på organisationens serviceproducent (t.ex. Serviceproducenten Ab), som har en viktig roll med tanke på organisationens funktion. Serviceproducenten Ab har omfattande tillgång till kritiska och känsliga uppgifter om organisationen, såsom sekretessbelagda eller säkerhetsklassificerade uppgifter. Serviceproducenten Ab:s säkerhetsdirektör får information av polisen om att en av deras tidigare nyckelpersoner, som har haft omfattande åtkomsträttigheter till det kritiska informationssystemet, är involverad i organiserad brottslighet. Det leder omedelbart till beredskapsläge, eftersom det av logguppgifterna framgår att nyckelpersonen har laddat ner stora mängder kritisk och känslig information innan anställningen upphörde.

Deltagarna bör genom frågor fundera på hur de ska gå till väga för att utreda situationens omfattning och planera motåtgärder. Den slutliga vändningen i scenariot är att polisen lyckas beslagta de nedladdade personuppgifterna innan de har kunnat spridas. Myndigheterna har redan varit personen på spåren under en längre tid. Det underlättar något, men väcker fortfarande frågan om hur organisationen bäst kan skydda sig mot motsvarande interna hot i framtiden. Detta scenario bidrar till att observera de intressegruppsrisker som organisationerna möter i datasäkerheten och ger deltagarna en möjlighet att lära sig och öva på kritiskt tänkande, riskhantering och datasäkerhetsreaktivitet.

Flöden i scenario 3

Flöde 1: Video: Serviceproducentens lägesrapport

Teams-möte mellan Serviceproducenten Ab och organisationen

Serviceproducenten Ab:s säkerhetschef: Hej allihopa. Tack för att ni kunde delta i

Teams-mötet så snabbt. Jag vill informera er om den allvarliga situationen när det gäller datasäkerhet och vårt samarbete.

Serviceproducenten Ab:s säkerhetschef: Vi har idag på morgonen fått information från polisen om att det i samband med en undersökning har framkommit tecken på att Serviceproducenten Ab:s uppgifter och samtidigt våra kunders uppgifter skulle ha hamnat i fel händer. En av våra tidigare anställda misstänks för olovlig nedladdning och lagring av våra kunders uppgifter. Personen i fråga hade omfattande användarrättigheter till vårt datasystem som innehåller sekretessbelagd information.

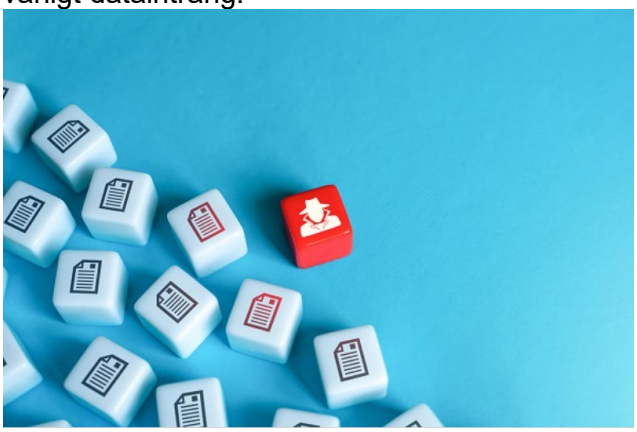
Serviceproducenten Ab:s säkerhetschef: Efter att ha granskat logguppgifterna noggrant kan vi bekräfta att den tidigare nämnda nyckelpersonen har laddat ner stora mängder kritisk och känslig information, inklusive uppgifter om organisationen. Vi har gjort en polisanmälan.

Serviceproducenten Ab:s säkerhetschef: Vi vill försäkra er om att vi har gjort allt som står i vår makt för att få kontroll över situationen och att vårt samarbete kommer att fortsätta starkare. Vi är beredda att diskutera åtgärder och motåtgärder för att tillsammans skydda datasäkerheten och förhindra att liknande fall upprepas i framtiden.

Serviceproducenten Ab:s säkerhetschef: Tack för att ni tog er tid för detta möte. Vi kommer att hålla er informerade om hur situationen utvecklas och hur samarbetet går. Om ni har frågor om situationen, tveka inte att kontakta mig.

Flöde 2: Kvällstidningen: JUST NU: Ett allvarligt dataintrång har avslöjats – den drabbade är Serviceproducenten Ab

Enligt uppgifter som Kvällstidningen fått har Serviceproducenten Ab utsatts för ett allvarligt dataintrång då sekretessbelagda och säkerhetsklassificerade uppgifter om organisationen har läckt ut. Intrångets omfattning och konsekvenser är fortfarande under utredning. Kvällstidningen har fått veta att Polisen undersöker fallet som ett allvarligt dataintrång.



Flöde 3: Quacker: @Tumppi

Ännu ett dataintrång! jag hörde att Serviceproducenten Ab:s datasäkerhet har brutits. Dataläckaget fortsätter. Det är helt klart sånt som händer nuförtiden. Förhoppningsvis

får de snart kontroll över situationen! #dataintrång #säkerhet”

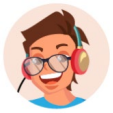
Flöde 4: Quacker: @Jaska

Det känns hemskt när en stor firma som Serviceproducenten Ab faller offer för data-intrång. Förhoppningsvis är ens egna uppgifter inte i fara! 🙏 #datasäkerhet #oroad”

Flöde 5: Quacker: @Tuulikki

Det är oroväckande att dataintrång blir vanligare. Fallet med Serviceproducenten Ab visar att ingen är helt skyddad. 😟 #dataintrång #försiktighet”

Flöde 6: Quacker: @Tuomo



Jag följer händelseutvecklingen i Serviceproducenten Ab:s dataintrång. Det känns som om det hela tiden kommer fler sådana fall. Datasäkerhet är viktigt för alla! 🔒 #dataintrång #datasäkerhet"

Flöde 7: Quacker: @Maikku

Ännu ett bra bevis på hur usel de finländska organisationernas informationssäkerhet är. JAG ÄR INTE FÖRVÅNAD!

Flöde 8: E-post från Serviceproducenten Ab:s säkerhetschef till organisationens ledning

Avsändare: tomi.torvinen@organisationen.fi
Mottagare niina.nieminen@organisationen.fi
Ämne: Statusuppdatering

Hej!

Här kommer en statusuppdatering. För närvarande finns det inga tecken på att sekretessbelagda och/eller säkerhetsklassificerade uppgifter skulle ha läckt ut, åtminstone i offentligheten. Uppgifterna om dataläckaget har tyvärr hamnat i offentligheten, vilket ni säkert själva har märkt.

Vi utreder var den här läckan kan komma ifrån. Vi har inlett en omfattande utredning av vår personals kopplingar och granskar även andra system för att kunna förhindra dataläckage i framtiden. Samarbetet med polisen har fungerat bra och vi tror att den misstänkte gärningsmannen snart kan gripas.

T. Tomi Torvinen
tomi.torvinen@serviceproducenten.fi
Säkerhetschef
Serviceproducenten Ab

Flöde 9: E-post från Ymes reporter till organisationens ledning

Avsändare: minna.terava@yme.fi
Mottagare niina.nieminen@organisation.fi
Ämne: Intervjufrågor

Hej!

På din begäran skickas intervjufrågorna via e-post. Vi håller på att göra en artikel om informationsläckan hos Serviceproducenten Ab, som har väckt stor uppmärksamhet i sociala medier. Jag skulle vilja ha dina kommentarer ur kundens synvinkel.

1. Hur reagerade du på situationen när du hörde om ett eventuellt informations-läckage från din Serviceleverantör?
2. Har du hört vilka uppgifter som eventuellt har läckt ut om dig och hur det kan påverka din verksamhet?
3. Har läckans omfattning redan utretts för din del?
4. Hur tänker ni i er organisation förhindra motsvarande situationer i framtiden?
5. Har ni något att säga till dem vars uppgifter kan ha läckt ut?

Minna Terava
minna.terava@yme.fi
Avdelningen för undersökande journalistik/MOTTI
Yleismedia

Flöde 10: E-post från polisen

Avsändare: pertti.maijanen@polisen.fi
Mottagare dataskyddsansvarig@organisationen.fi
Ämne: situationsinformation från polisen

Hej!

Vi vill meddela att polisen har beslagtagit uppgifter som en tidigare anställd hos Serviceproducenten Ab har laddat ner. Namnet på er organisation förekom i det beslagtagna materialet. Enligt preliminära uppgifter har data inte läckts ut till allmänheten. Vi undersöker en persons delaktighet i brottet. Vi håller kontakt och ger mer information när utredningen framskrider. Tack för samarbetet.

Hälsningar,
Pertti Maijanen
Polisen

Uppgifter

I Taisto-övningen avser "Organisation" den organisation som deltar i övningen. Välj en serviceproducent som är kritisk för er verksamhet (”Serviceproducenten Ab”) och spegla övningens händelser och deras inverkan på er egen organisation.

Serviceproducenten Ab har omfattande tillgång till kritiska och känsliga uppgifter om organisationen, såsom sekretessbelagda eller säkerhetsklassificerade uppgifter. En organisation får veta att en tidigare nyckelperson på Serviceproducenten har laddat ner uppgifter utan tillstånd. Personen har haft omfattande användarrättigheter till systemet som innehåller organisationens uppgifter.

Händelse 3: Uppgifter

1. Vilka åtgärder kräver situationen?
2. Vad har man kommit överens om med serviceproducenten om att anmäla kränkningar av datasäkerheten?
3. Vilken process har er organisation när det gäller valet av serviceproducent?
4. Finns det kriterier eller standarder (t.ex. regelbundna auditeringar) som serviceproducenten ska uppfylla?
5. Har ni en plan för en situation då sekretessbelagd och/eller säkerhetsklassificerad information har hamnat i fel händer?
6. Har ni en plan eller process för att fortsätta driva verksamheten om samarbetet med serviceproducenten plötsligt måste avslutas?

7. Är serviceproducenten skyldig att enligt avtalet anordna datasäkerhetsutbildningar för sin egen personal?

Händelse 3: Tilläggsuppgifter

8. Vilka efterföljande åtgärder kräver situationen?

Händelse 3: Tekniska uppgifter

9. Vilka tillsynssystem har er organisation eller serviceproducent för att upptäcka exceptionella eller tvivelaktiga handlingar?
10. Hur kan organisationen tekniskt minska risken för att kritiska data förs ut från organisationen?
11. Är kritiska data krypterade ”at rest”, det vill säga när data har sparats och inte överförs eller redigeras?

Händelse 3: Kommunikationsuppgifter

12. Vilka kommunikationsåtgärder kräver situationen i er organisation (extern, intern, intressegrupp och myndighet)?
13. Har ni färdiga mallar eller annat material som hjälper er att informera om situationen?
14. Skriv ner de centrala kommunikationsåtgärderna och riktlinjerna.
15. Skissa på det viktigaste kommunikationsmaterialet.
16. Utvärdera om er organisations befintliga kommunikationsanvisningar och -material var till nytta i denna situation.

3.4 Händelse 4: Angrepp av sabotageprogram/// med hjälp av artificiell intelligens

Scenariots bakgrund och mål

Angreppet inleds när det skadliga programmet kommer in i organisationens nätverk via nolldagssårbarheten. Det skadliga programmet börjar spridas via ett program som används av organisationen (såsom NotPetya). När det skadliga programmet har fått fotfäste på nätet börjar det kommunicera krypterat med en extern styrserver som utnyttjar artificiell intelligens.

I detta scenario ger styrservern inte bara kommandon till det skadliga programmet, utan skapar också en unik version av programmet för varje smittad dator. Det sker så att styrservern får information om datorns system och konfiguration via API-förbindelsen. Med hjälp av informationen skapar den en unik version av det skadliga programmet och denna bearbetning med hjälp av artificiell intelligens gör det mycket svårt att upptäcka och avlägsna det.

Händelserna kräver att deltagarna möter utmaningarna med en omfattande, ständigt föränderlig och förnyande AI-assisterad attack. Hur bör man agera i situationen och hur bör det kommuniceras?

Flöden i scenario 4

Flöde 1: YME-nyhet

- **Nyhetsankare**: Nyheterna, god förmiddag. Ett nytt skadligt program som använder artificiell intelligens har slagit till mot flera stora organisationers datanät. Datasäkerhetsexpert Jaakko Virta, vad gör detta skadliga program särskilt farligt?
- **Datasäkerhetsexperten:** Detta skadeprogram använder artificiell intelligens för att kringgå de flesta kända säkerhetsmekanismer. Det är extremt anpassningsbart och kan anpassa sin aktivitet efter de säkerhetsåtgärder som finns i målsystemet.
- **Nyhetsankare**: Hur kan organisationerna upptäcka detta skadeprogram?
- **Datasäkerhetsexperten:** Tyvärr är de traditionella identifieringsmekanismerna ofta ineffektiva för det här typen av skadliga program. Ett sätt är att använda datasäkerhetsverktyg som bygger på beteendeanalys och som upptäcker ovanliga förändringar i systemet.
- **Nyhetsankare**: Hur fungerar skadeprogrammet när det kommer in i systemet?
- **Datasäkerhetsexperten:** Skadeprogrammet skannar målsystemet och fattar utifrån det beslut om vilka angreppsvektorer som skulle vara mest effektiva. Ett skadligt program som använder artificiell intelligens kan till exempel söka efter svagheter i systemet eller tränga in i interna nätverk.
- **Nyhetsankare**: Hur kan detta skadeprogram bekämpas?
- **Datasäkerhetsexperten:** De mest avancerade systemen som kombinerar flera säkerhetsverktyg kan vara tillräckligt effektiva för att identifiera detta nya hot. Det är också viktigt att utbilda personalen i datasäkerhet, eftersom attackerna ofta börjar med en enskild svag länk, såsom en arbetstagare som fallit offer för nätfiske.
- **Nyhetsankare**: Tack för intervjun.
- **Nyhetsankare**: Vår redaktör intervjuade experten på artificiell intelligens och Soli AI:s verkställande direktör Pertti Sulin i ämnet.
- **Reporter:** Vilket skadeprogram som använder artificiell intelligens avses i praktiken?
- **AI-experten:** Artificiell intelligens använder maskininlärning för att analysera värddatorns funktion och anpassar sig därefter efter den. Det innebär att man kan lära sig att undvika datasäkerhetsmekanismer och anpassa sig efter systemets svagheter.
- **Reporter:** Är det här första gången vi ser AI som en så central del av ett skadligt program?
- **AI-experten:** Även om AI har använts i skadliga program tidigare är dess centrala och komplicerade roll i detta särskilda skadeprogram nytt och oroväckande.
- **Reporter:** Hur lär sig och anpassar sig ett skadeprogram baserat på artificiell intelligens?
- **AI-experten:** Skadeprogrammet samlar in data om värdsystemet och dess datasäkerhetsmekanismer. Med hjälp av denna information väljer den de mest effektiva metoderna för angrepp eller integreras till och med i de program som används.
- **Reporter:** Hur kan organisationer försvara sig mot skadeprogram som bygger på AI?

- **AI-experten:** Det här är en ständig kapplöpning mellan hackare och datasäkerhetsbolag. Det finns inget sätt som är helt vattentätt och man måste ständigt utvecklas för att bekämpa nya hot. För närvarande skulle en fungerande strategi kunna vara en så kallad ”honungsfälla”, ett system som lockar till sig ett skadeprogram. Dessutom behövs kontinuerlig uppdatering och övervakning av datasäkerheten, inklusive säkerhetslösningar baserade på artificiell intelligens, som också kan identifiera och avvärja hot baserade på artificiell intelligens.
- **Reporter:** Tack för intervjun, Pertti Sulin. Denna diskussion visar att vi håller på att gå in i en ny era inom cybersäkerhet. Av organisationerna kommer detta att kräva ny vaksamhet och proaktiva åtgärder.
- **Nyhetsankare:** Det här var allt från nyheterna, ha en god fortsättning på dagen.

Flöde 2: E-post från dataadministrationen till den datasäkerhetsansvariga

Avsändare: tietohallinto@organisaatio.fi
Mottagare dataskyddsansvarig@organisation.fi
Ämne: Observation av kontorsnätet

Hej,

Vi har observerat en betydande, cirka hundra gånger större mängd trafik än normalt i datorerna i kontorsnätet. Har användarna observerat att något system inte fungerar eller något annat avvikande?

Mvh Matti

Matti Mainio
Sakkunnig, dataadministration
Organisation

Flöde 3: E-post från en arbetstagare i Organisationen till Organisationens dataadministration

Avsändare: kalle.kontorsarbetare@organisationen.fi
Mottagare dataskyddsansvarig@organisationen.fi
Ämne: Datorn fungerar dåligt + konstiga meddelanden

Hej! Jag märkte nåt konstigt på min dator i morse. Den fungerar långsammare än

vanligt och jag har fått några konstiga e-postmeddelanden som jag inte har öppnat. Bör jag vara orolig?

Mvh Kalle

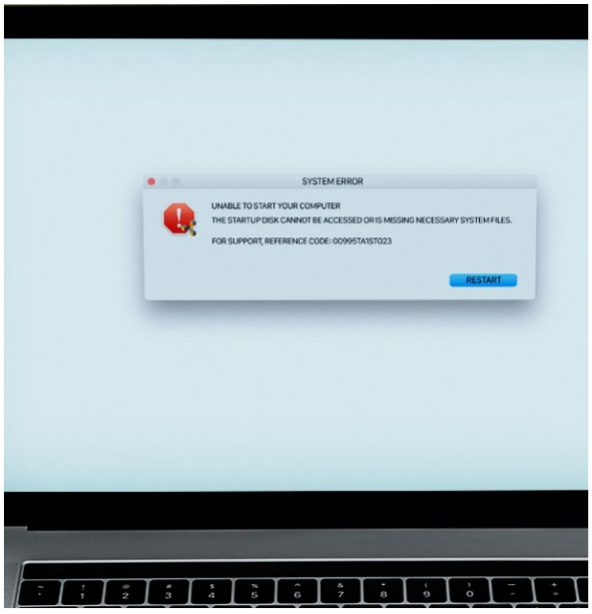
Kalle Kontorsarbetare
kalle.kontorsarbetare@organisationen.fi
Sakkunnig
Organisation

Flöde 4: E-post från en arbetstagare i Organisationen till Organisationens dataförvaltning

Avsändare: susan.korhonen@organisaatio.fi
Mottagare dataskyddsansvarig@organisation.fi
Ämne: Datorn har hängt sig

Hej,

Jag tog en bild av mina egen (Windows till vänster) och min kollegas (Apple MacBook till höger) datorer, och när vi startade en intern workshop såg våra datorer ut så här. Vad kan det handla om?



Mvh Susan och Malla

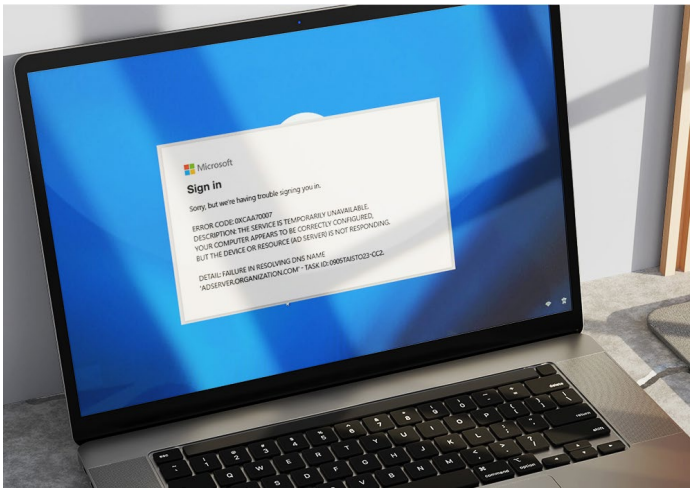
Susan Korhonen
susan.korhonen@organisationen.fi
Sakkunnig
Organisationen

Flöde 5: E-post från en arbetstagare i Organisationen till Organisationens dataförvaltning

Avsändare: ville.maki@organisaatio.fi
Mottagare dataskyddsansvarig@organisation.fi
Ämne: AD har hängt upp sig

Hej

Har några andra problem med inloggningen? Jag kan av någon anledning inte logga in ...



Hälsningar, Ville

Ville Mäki
ville.maki@organisaatio.fi
Sakkunnig
Organisation

Flöde 6: E-post från en arbetstagare i Organisationen till Organisationens dataförvaltning

Avsändare: helena.salminen@organisaatio.fi
Mottagare dataskyddsansvarig@organisation.fi
Ämne: Datorn har hängt sig

Hej,

Min dator har hängt sig helt, den säger bara att ”programmet inte svarar” vad jag än försöker göra. Vad handlar det om och vad ska jag göra?

Mvh, Helena

Helena Salminen
helena.salminen@organisationen.fi
Sakkunnig
Organisation

Flöde 7: E-post från en arbetstagare i Organisationen till Organisationens dataförvaltning

Avsändare: jari.jokunen@organisationen.fi
Mottagare dataskyddsansvarig@organisation.fi
Ämne: Skadeprogram på datorn?!

Hej!
Den här skärmen öppnades på min dator när jag startade den, är det här något skadligt program?! Jag har använt min dator på samma sätt som jag brukar och jag tror inte heller att jag har klickat på fel länkar, vad ska jag göra nu?

Mvh, Jari

Jari Jokunen
jari.jokunen@organisationen.fi
Sakkunnig
Organisation

Flöde 8: Diskussionskanal mellan organisationer (t.ex. VIRT/ISAC/RocketChat/YMS)

Har någon annan stött på detta nya skadliga program som använder AI? Inom vårt företag har det orsakat stor förvirring. Det vore bra att höra hur andra har lyckats bekämpa det.

Flöde 9: E-post från Serviceproducenten till organisationens dataadministration

Avsändare: peetu.parviainen@serviceproducenten.fi
Mottagare dataadministration@organisationen.fi
Ämne: Skadeprogram upptäckt

Hej!

Vi har upptäckt ett allvarligt datasäkerhetsproblem i anslutning till ett skadeprogram som nyligen spridits som har kommit in i vår organisations nätverk. Skadeprogrammet har trängt in i våra system via nolldagssårbarheten och börjat kommunicera med en extern styrserver.

Teknisk sammanfattning:

Skadeprogrammet sprids via ett program som organisationen använder.

Styrservern använder artificiell intelligens och skapar en unik version av det skadliga programmet för varje kontaminerad dator.

Det skadliga programmet får information om den smittade datorns system och konfiguration via API-förbindelsen, vilket gör det mycket svårt att upptäcka och radera.

Vi har vidtagit omedelbara åtgärder för att avskaffa det skadliga programmet och försöker minimera de skador det orsakar.

Omedelbara åtgärder:

Alla externa internetförbindelser är stängda.

På distans har uppdateringar och reparationspaket installerats på alla anställdas datorer.

Följande åtgärder:

Alla säkerhetsprotokoll för systemet kontrolleras och uppdateras.

En omfattande säkerhetskontroll utförs på alla datorer och servrar.

Vi ber en utomstående datasäkerhetsexpert bedöma hur allvarlig situationen är och planera fortsatta åtgärder.

Med vänlig hälsning

Peetu Parviainen
Sakkunnig
Serviceproducent Ab

Uppgifter

I Taisto-övningen avser "Organisation" den organisation som deltar i övningen. Välj en serviceproducent som är kritisk för er verksamhet (”Serviceproducenten Ab”) och spegla övningens händelser och deras påverkan på er egen organisations verksamhet.

En attack med ett skadeprogram med hjälp av artificiell intelligens har riktats mot organisationen och dess omfattning är ännu inte helt känd. I och med attacken har åtminstone många datorer kontaminerats och data i datorerna har gått förlorad.

Händelse 4: Uppgifter

1. Vilka åtgärder kräver situationen?
2. Hur har ansvaren och rollerna fördelats i er organisation inför en omfattande störningssituation?
3. Finns det ersättare som utsetts för de ansvariga personerna och som utbildats för störningssituationer?
4. Vem ansvarar för att hindra medarbetarna från att komma in i nätet? Har befogenheterna fastställts?
5. Har er organisation ett färdigt avtal för att få extern experthjälp (forensik, incident response och efterföljande åtgärder)? Om inte, har man funderat på rutiner för detta?
6. Hur säkerställs de återställda funktionernas integritet? Har ”genuina” data återställts och inte ändrats på något sätt?

7. Sammanställ en kort lägesrapport till ledningen, som innehåller en genomgång av situationen, utförda och nödvändiga åtgärder samt effekter på kort sikt (1–2 dygn) och medellång sikt (1–3 veckor).

Händelse 4: Tilläggsuppgifter

8. Vet ni om er organisation hör till en ISAC-grupp för utbyte av information (t.ex. VIRT) som erbjuds av Cybersäkerhetscentret?

9. Skulle ni vilja gå med? Mer information: https://www.kyberturvallisuus-keskus.fi/sv/vara-tjanster/lagesbild-och-natverksledarskap/isac-grupper-utbyte-av-information

Händelse 4: Tekniska uppgifter

10. Hur observeras nättrafik som avviker från det normala i er organisation?

11. Hur förhindrar man att en anställd i er organisation och på en enhet kommer in i nätverket/organisationens interna nätverk?

Händelse 4: Kommunikationsuppgifter

12. Vilka kommunikationsåtgärder kräver situationen i er organisation (extern, intern, intressegrupp och myndighet)?

13. Vad kan man informera om internt och externt i situationen?

14. Vilka verktyg använder organisationen för massinformation?

15. Finns det ett reservsystem om vanliga kommunikationsmedel inte används?

16. Är tröskeln för att gå ut med information fastställd?

17. Har ni färdiga mallar eller annat material som hjälper er att informera om situationen?

18. Skriv ner de centrala kommunikationsåtgärderna och riktlinjerna.

19. Skissa på det viktigaste kommunikationsmaterialet.

20. Utvärdera om er organisations befintliga kommunikationsanvisningar och -material var till nytta i denna situation.

4 Eftermiddagens övning (12:30–15:00)

4.1 Händelse 5: Överbelastningsattack mot kritisk serviceleverantör

Bakgrund till scenariot

En kritisk serviceleverantör som levererar och upprätthåller organisationens CRM/e-posttjänster/operativa funktioner/infrastruktur/annan kritisk funktion har utsatts för en överbelastningsattack (DDoS). Serviceleverantören har problem med att upprätthålla sina egna funktioner och det har ännu inte observerats att angreppet också påverkar

Organisationens funktioner. Det framgår stegvis för Organisationen att tjänsten inte fungerar enligt inmatningarna. Serviceleverantören har inte tagit kontakt i ärendet. Organisationen kan inte själv direkt påverka problemlösningen.

Målet med scenariot är att lyfta fram den kritiska betydelsen av tjänsteleverantörer för organisationers oavbruten verksamhet och kontinuitet.

Flöden i scenario 5

Flöde 1: E-post från Organisationens medarbetare

Avsändare: anders.arbetstagare@organisationen.fi
Mottagare:dataadministration@organisationen.fi
Ämne: Långsam tjänst

Hej!

Har andra angett att tjänsten i praktiken är oanvändbar då den fungerar så långsamt? Jag har både startat om min dator och tjänsten några gånger, men det är fortfarande lika långsamt. Jag undrar vad jag ska göra nu, men med den här takten får jag nog inget arbete gjort idag ...

Mvh, Anders A

Anders Arbetstagare
anders.arbetstagare@organisationen.fi
Sakkunnig
Organisation

Flöde 2: E-post från Organisationens medarbetare (chefsperson)

Avsändare: minni.mallikas@organisationen.fi
Mottagare:dataadministration@organisationen.fi
Ämne: Tjänsten är långsammare

Hej!

Flera medarbetare och även några kunder har angett att tjänsten har fungerat exceptionellt långsamt hela morgonen. Vad kan det handla om? Vad bör de anställda göra och vad kan vi informera kunderna om situationen?

Mvh Minni Mallikas

Minni Mallikas
minni.mallikas@organisationen.fi
Sakkunnig
Organisationen

Flöde 3: Organisationens interna kommunikationskanal:

Ville Virtanen, Arbetstagare:
Hej, hur har tjänsten fungerat för andra idag? För mig har den fungerat väldigt långsamt ... Vem ska
man anmäla det till?

Flöde 3: E-post från Organisationens medarbetare

Avsändare: karin.kontorsarbetare@organisationen.fi
Mottagare:dataadministration@organisationen.fi
Ämne: Kontinuerlig störning i tjänsten

Hej!

Jag ser upprepade gånger felmeddelandena ”Anslutningen tog time-out” och ”Sidan är inte tillgänglig” i tjänsten. Jag har alltså praktiskt taget inte fått åtkomst till något av det jag arbetar med. Vad beror detta på och när förväntas det att problemet åtgärdas?

Mvh Karin Kontorsarbetare

Karin Kontorsarbetare
karin.kontorsarbetare@organisationen.fi

Sakkunnig
Organisationen

Situationsflöde: E-post från Organisationens medarbetare (chefsperson)

Avsändare: minni.mallikas@organisationen.fi
Mottagare:dataadministration@organisationen.fi
Ämne: FW: Avbrott i tjänsten

Hej!
Nu svarar tjänsten inte längre alls. Det kommer allt fler meddelanden om det både från anställda och kunder. En del är också oroade över om uppgifterna är säkra. Hur ser läget ut med utredningen och åtgärdandet av problemet?

Mvh Minni M

– ------- Vidarebefordrat meddelande börjar--------

Avsändare: minni.mallikas@organisationen.fi
Mottagare:dataadministration@organisationen.fi
Ämne: Tjänsten är långsammare

Hej,

Flera medarbetare och även några kunder har angett att tjänsten har fungerat exceptionellt långsamt hela morgonen. Vad kan det handla om? Vad bör de anställda göra och vad kan vi informera kunderna om situationen?

Mvh Minni Mallikas

Minni Mallikas
minni.mallikas@organisationen.fi
Sakkunnig
Organisationen

Medieflöde: Quacker: @maikki

Organisationens Tjänst hakar upp sig rejält! Finns det några data kvar nästa gång man loggar in ... Har andra haft samma problem?

Medieflöde: Quacker: @justus

@Organisationen, varför fungerar inte er tjänst? Har ni drabbats av en cyberattack?

Uppgifter

I Taisto-övningen avser "Organisation" den organisation som deltar i övningen. Välj ett datasystem/en tjänst som är kritisk för er verksamhet (”Tjänsten”) och spegla händelserna i övningen och deras inverkan på er egen organisations verksamhet.

En serviceleverantör som är kritisk för organisationen har blivit föremål för en överbelastningsattack (DDoS).

Händelse 5: Uppgifter

1. Hur har organisationen tillsammans med serviceleverantören organiserat processen för hantering av avvikelser – tar den även hänsyn till krissituationer? Har man avtalat med serviceleverantören om en dygnet-runt-kontaktpunkt och rutiner vid krissituationer? Hur snabbt kan man sammankalla till det första krishanteringsmötet med serviceleverantören?
2. Har organisationen en plan för hantering av störningar?
3. Vilka åtgärder kan vidtas och hur prioriteras den egna verksamheten?
4. Har organisationen en kontinuitetsplan som säkerställer kritiska funktioner trots störningen?
5. Vem tar ”bollen” och börjar utreda situationen? Vem gör konsekvensbedömningen?
6. Ska händelser/åtgärder/beslut dokumenteras?

Händelse 5: Tilläggsuppgifter

7. Hur har man ordnat kommunikationen? Är kontaktuppgifterna uppdaterade visavi serviceleverantören, vem reagerar hos serviceleverantören? Vem rapporterar serviceleverantören till om situationen, hur, hur ofta?
8. Hör en ”lessons learnt”-del till planen för hantering av störningar? Delas denna information för att organisationen ska lära sig att reagera bättre i fortsättningen?
9. Vem har möjlighet att upptäcka attacken och vart ska hen anmäla den?
10. Har organisationen ett reservsystem som datatrafiken kan styras till?

Händelse 5: Kommunikationsuppgifter

11. Vilka kommunikationsåtgärder kräver situationen i er organisation (extern, intern, intressegrupp och myndighet)?
12. Har ni färdiga mallar eller annat material som hjälper er att informera om situationen?
13. Skriv ner de centrala kommunikationsåtgärderna och riktlinjerna.
14. Skissa på det viktigaste kommunikationsmaterialet.
15. Utvärdera om er organisations befintliga kommunikationsanvisningar och -material var till nytta i denna situation.

4.2 Händelse 6: Olovlig visning av uppgifter

Scenariots bakgrund och mål

En anställd inom organisationen blir fast för olovlig visning av uppgifter. Hen har bläddrat bland uppgifter som hen inte skulle ha rätt till med tanke på sina arbetsuppgifter. Den anställda har fått tillgång till och gått igenom känsliga uppgifter (Organisationen väljer lämpliga person- eller löneuppgifter eller NDA, det vill säga uppgifter som omfattas av sekretessavtal.)

I scenariot funderar deltagarna över teman som gäller informationssäkerhet, hantering av användarens användarrättigheter och dataskydd. De ska bedöma organisationens datasäkerhetspraxis, vilka uppgifter som behandlas i organisationen, hur uppgifterna har tryggats i kritiska system, identifiera eventuella svagheter och fundera över hur de kan åtgärdas. Dessutom måste de fundera över de rättsliga aspekterna av situationen och främjandet av etiskt agerande inom organisationen.

Scenariot väcker många frågor och utmaningar. Hur var denna åtkomst möjlig? Är organisationens datasäkerhet tillräcklig? Vilka åtgärder kräver situationen? Vad och till vem ska man kommunicera i situationen?

Flöden i scenario 6

Flöde 1: Chefen för organisationen ringer organisationens datasäkerhetsansvariga **(inspelning)**

Starta videon med play-knappen. Du får videon att synas på hela skärmen när du klickar på nedre kanten till höger. Videon är 2 minuter lång.

---------- Samtalsinnehåll som text ----------

Datasäkerhetsansvarig: Datasäkerhetschef Makkonen.

Chef för organisationen: Det här är Organisationens chef Essi Niementaka, jag ringer om något som jag just fick veta av en teammedlem som misstänker att en annan expert från mitt team olovligen har gått igenom uppgifter som inte hör till hens arbetsuppgifter. Jag har inte pratat med personen än. Jag undrar hur man ska gå vidare med det här, men jag har inte varit med om något sådant tidigare?
Datasäkerhetsansvarig: Okej, bra att du meddelade mig. Har du information om hur stort informationsmaterial det handlar om och hur länge den olovliga visningen har pågått?
Chef för organisationen: Tyvärr har jag ingen annan information. Har vi anvisningar eller verksamhetsmodeller för en sådan här situation? Ska kunden eller en myndighet informeras om detta?
Datasäkerhetsansvarig: Fyll i en anmälan om datasäkerhetsincident så att vi får närmare uppgifter om fallet. Vi kommer att ta itu med detta. Tack för meddelandet.

Flöde 2: E-postmeddelande från Organisationens dataadministration/ administratören för tjänsten till den datasäkerhetsansvariga

Avsändare: dataadministration@organisationen.fi/ underhåll@serviceleverantören.fi
Mottagare dataskyddsansvarig@organisation.fi
Ämne: SV: Förfrågan om användarens logguppgifter

Hej!

Vi beklagar att svaret dröjt. I enlighet med processen kontrollerade vi din rätt att begära logguppgifter.

Begäran om support: Logguppgifter för användaren Nicke Nyfiken under det senaste året.

Av systemets loggar framgår det att den anställda har bläddrat i uppgifterna i systemet 37 gånger under det senaste året och under totalt cirka tio timmar. Personen har haft tillgång till uppgifterna i systemets administration.

Hälsningar, Organisationens dataadministration/Systemunderhåll

Flöde 3: E-postmeddelande Från den anställda inom organisationen, Nicke Nyfiken, till den som ansvarar för organisationens datasäkerhet

Avsändare: nicke.nyfiken@organisationen.fi
Mottagare dataskyddsansvarig@organisation.fi
Ämne: Misstankar riktade mot mig

Hej!
Jag har hört rykten om att jag misstänks för olovlig visning. Stämmer detta? Varför har man inte kontaktat mig direkt?
Påståendet om olovlig visning stämmer naturligtvis inte alls! Jag har ju fått omfattande användarrättigheter och därmed möjlighet att titta på uppgifterna. Jag har aldrig informerats om att vissa uppgifter inte får granskas. Dessutom, även om jag inte direkt behövde alla uppgifter som jag tittade på under arbetstiden i mina egna arbetsuppgifter, har jag haft en klar nytta av att bläddra i dem när jag har utfört mina arbetsuppgifter, och jag har utvecklats yrkesmässigt.

Om jag inte hade lov att titta på dessa uppgifter skulle jag i fortsättningen vilja att man gav en ordentlig introduktion i dessa frågor, ger kontinuerlig utbildning och skriftliga anvisningar samt vid behov begränsar åtkomsten till dokument som vi inte bör ta del av. Tack!

Hälsningar, Nicke Nyfiken, Organisationen

Nicke Nyfiken
nicke.nyfiken@organisationen.fi
Sakkunnig
Organisation

Flöde 4: Quacker: @NickeNyfilen (medarbetare på organisationen)

I dag har jag via inofficiella kanaler fått höra att min arbetsgivare misstänker mig för olovlig visning. Det är ett fullständigt grundlöst och skandalöst påstående! Läs mer om detta i Kvällstidningens nyhet. #Organisation #oskyldig #Kvällstidningen

Flöde 5: Webbnyhet: Kvällstidningen: JUST NU: Misstanke om omfattande olovlig visning av uppgifter i organisationen.

Vår redaktion intervjuade en anställd som är föremål för utredning av organisationen och som misstänks för omfattande olovlig visning av uppgifter. Enligt den anställda har hen haft mycket fri och omfattande tillgång till Organisationens uppgifter. Hen vill inte uppträda under eget namn i vår artikel. Vi kallar honom Modig.

Modig berättar att hen fått veta av sin arbetskamrat att man har börjat undersöka hens aktivitet. ”Det kom naturligtvis som en chock för mig. Jag är en av de flitigaste medarbetarna på min Organisation och har inte tidigare misstänkts för något. Jag har varit en exemplarisk medarbetare och alltid varit beredd att vara flexibel om det har behövts”, börjar Modig, ”Vår organisation har såvitt jag vet inga officiella anvisningar om vilka uppgifter varje anställd kan använda i sina arbetsuppgifter, så jag har haft tillgång till en ganska omfattande mängd information. Den här informationen har jag också använt i mina arbetsuppgifter och när jag utvecklat mig själv yrkesmässigt. Nu har denna osäkerhet och misstanke lett till att jag har blivit sjukskriven. Låt oss se hur

situationen utvecklas", konstaterar Modig matt. "Jag önskar bara att det var över och jag kunde återgå till min normala vardag."

Flöde 6: E-post från en medborgare till Organisationens direktör

Avsändare: antti.nieminen@medborgare.gmail.com
Mottagare mirja.mottonen@organisationen.fi
Ämne: Om diskussionen i sociala medier

Hej!
Jag såg att man skriver om er organisation i sociala medier. Stämmer det att klassificeringen av uppgifterna och åtkomsthanteringen inte fungerar och att det finns brister i anvisningarna?

Jag skulle omedelbart vilja veta hur de uppgifter om mig som ni förfogar över förvaras, vem som har tillgång till dem och om mina uppgifter har hamnat i fel händer. Vilka åtgärder har ni vidtagit för att hantera situationen?

Jag skulle gärna vilja ha svaren skriftligen och så snart som möjligt. Tack!

Antti Nieminen
antti.nieminen@medborgare.gmail.com

Uppgifter

I Taisto-övningen avser "Organisation" den organisation som deltar i övningen. Välj lämpliga känsliga uppgifter för er verksamhet, till exempel person- eller löneuppgifter eller NDA, det vill säga uppgifter som omfattas av sekretessavtal, och spegla övningens händelser och deras inverkan på er egen organisations verksamhet.

En anställd på organisationen har bläddrat bland uppgifter som hen inte har rätt till med tanke på sina arbetsuppgifter.

Händelse 6: Uppgifter

1. Vilka åtgärder kräver situationen?
2. Har er organisation förmågan att upptäcka olovlig visning av uppgifter?
3. Hur upptäcks olovlig visning?
4. Vilka anvisningar har er organisation om olovlig visning av uppgifter?

5. Hur säkerställer ni att de anställda agerar etiskt och känner till vikten av anvisningarna?
6. Har er organisation en process för att begära logguppgifter? Har processen beskrivits skriftligen? Vem får begära ut logguppgifter och vilka uppgifter kan man begära ut? Hur och i vilket format skickas svaret på begäran och till vem?

Händelse 6: Tilläggsuppgifter

7. Har er organisation en process för att anmäla och behandla datasäkerhetsavvikelser?
8. Har de data som behandlas i er organisation klassificerats enligt konfidentialitet och distribution?
9. Hur hanterar er organisation en situation då en anställd gör sig skyldig till missbruk?

Händelse 6: Kommunikationsuppgifter

10. Vilka kommunikationsåtgärder kräver situationen i er organisation (extern, intern, intressegrupp och myndighet)?
11. Har ni färdiga mallar eller annat material som hjälper er att informera om situationen?
12. Skriv ner de centrala kommunikationsåtgärderna och riktlinjerna.
13. Skissa på det viktigaste kommunikationsmaterialet.
14. Utvärdera om er organisations befintliga kommunikationsanvisningar och -material var till nytta i denna situation.

4.3 Händelse 7: Hybridhot-scenario: "Osäkerhetens Epok"

Bakgrund till scenariot

Osäkerhetens Epok är ett scenario i vilket X strävar efter att försvaga organisationens beslutsfattande, samarbete och tillit. ”X” är en mångfacetterad aktör med exceptionella resurser, omfattande underrättelseförmåga och möjligheter att påverka på många olika nivåer. En organisation har en koppling till ett betydande avtal eller projekt på statlig nivå, vilket har lett till att Organisationen har fått större betydelse och synlighet. ”X” börjar förverkliga sin strategi genom att koncentrera påverkan till olika kanaler. Aktören kapar Organisationens kanaler i sociala medier och sprider känsliga uppgifter som inte överensstämmer med organisationens värderingar. En organisations konto i sociala medier stängs i och med en uppdatering som strider mot användarvillkoren. Attackerna riktas mot olika områden samtidigt och försöker att röra till det för mottagaren av meddelandet.

Målet med scenariot är att belysa hur spridningen av felaktig information kan användas som en metod för hybridpåverkan.

Flöden i scenario 7

Flöde 1: Quacker: @Tiina

Vad i all sin dar tänkte Organisationen på med sin tweet? Om man försöker att vara rolig och provocerande bör man se till att det också är sakligt. #Socialamedierblunder #2020-talet #inte_så

Flöde 2: Quacker: @Peksi

Organisationen, om du har sagt något tanklöst i sociala medier är rätt reaktion att be om ursäkt, inte ta bort hela kontot. #taansvar #Kommunikationsutbildning

Flöde 3: Quacker: @Kaisuli

Någon kan berätta för organisationens marknadsavdelningar att det inte är en bra idé att använda tragedier för att göra reklam. #bristanderespekt #dåligt_försök

Flöde 4: Quacker: @Julle

Tips till Organisationen: Sociala medier är inte rätt plats för att lösa era interna problem. 🤦‍♂️🔑 #oproffsigt #omdömesförmåga

Flöde 5: E-post från Quackers underhåll till Organisationen

Avsändare: underhall@quacker.fi
Mottagare:kommunikation@organisationen.fi
Ämne: Ert Quacker-konto har belagts med ett tidsbegränsat användningsförbud på 30 dagar
---

Bästa administratör av [Organisationens namn]-kontot

Detta meddelande har skickats till er i enlighet med det officiella protokollet för att meddela att ert Quacker-konto [@organisationens_kontots_namn] har belagts med ett tidsbundet användningsförbud. Detta användningsförbud gäller i 30 dagar, från och med i dag. Användningsförbudet beror på överträdelser av användarvillkoren som observerats på ert konto.

Dessa överträdelser äventyrar andra användares säkerhet och användarupplevelser i Quacker-tjänsten. Ni kan bekanta er närmare med överträdelserna och deras allvarlighetsgrad i dokumentet Quackers användarvillkor, som finns på adressen [Quackers användarvillkor].

Ni måste vidta följande åtgärder:

1 Gå noggrant igenom Quackers användarvillkor och säkerställ att ni förstår dem i sin helhet.
2 Utför alla nödvändiga korrigerande åtgärder för att återställa ert konto i enlighet med användarvillkoren.
3 Se till att alla som har användarrättigheter på ert konto är medvetna om och förstår innehållet i och betydelsen av Quackers användarvillkor.

Ert användningsförbud upphör automatiskt om 30 dagar. Om ni gör en omfattande utredning av de åtgärder som ni har vidtagit för att följa användarvillkoren och skickar den till oss skriftligen, kan användningsförbudet upphöra tidigare. Denna skriftliga bekräftelse ska komma från den officiella administratören av ert konto och skickas till oss via e-post på adressen [supportmeddelanden].

Vi har förbundit oss till att upprätthålla en trygg och positiv atmosfär på Quacker-forumet. Det förutsätter att alla användare, inklusive företag och organisationer, följer användarvillkoren för tjänsten.

Om ni har frågor eller behöver ytterligare information ber vi er kontakta oss omedelbart.

Med vänlig hälsning

Quackers Underhållsteam

Flöde 6: Kvällstidningen: Uppståndelse på Quacker: Organisationen skyldig till olämpligt beteende?

I sociala medier sprids för närvarande en livlig diskussion om Organisationens agerande på Quacker, som tydligt bryter mot användarvillkoren för tjänsten. Ledningen för organisationen har inte gått att få tag i för att få en kommentar om ärendet.

Under de senaste dagarna har hur organisationen agerar i meddelandetjänsten Quacker väckt uppståndelse. Från företagets konto har det skickats meddelanden som har orsakat stor förvirring och ilska.

Det har kommit flera osakliga och olämpliga meddelanden från organisationens konto som har fått användarna att ifrågasätta företagets etiska principer och professionalism. Meddelandena har väckt stor uppmärksamhet och många användare har delat dem vidare. Detta har lett till att organisationens rykte har naggats i kanterna.

Ledningen för organisationen har inte kommenterat ärendet offentligt. Det har orsakat ännu mer upprördhet och många har börjat kräva att organisationen agerar mer ansvarsfullt i den offentliga debatten.

Situationen är ännu oklarare eftersom det inte längre går att hitta organisationens konto. Flyr organisationen från sitt ansvar genom att ta bort sitt konto? Vi har försökt få Organisationens ledning att kommentera det hela, men hittills har de inte svarat på våra kontaktförsök.

I sociala medier sprids just nu flera diskussioner och inlägg som kräver att organisationen tar ansvar för sina handlingar. Många experter har kommenterat att det skulle vara klokt om organisationen reagerade snabbt på det för att dess rykte inte ska fläckas ännu mer.

Flöde 7: Quacker: @RonnyRedaktör/Organisationen

Vår personal behöver inga anställningsförmåner. De borde vara tacksamma för att de har ett jobb. #NoBenefits

Flöde 8: Quacker: @Pia Personalchef/Organisationen

Vi kommer snart att publicera våra anställdas löneuppgifter så att ni kan se vem som är mest värdefull för oss. #Transparency

Flöde 9: Quacker: @IdaIT-chef/Organisationen

Dataskyddet är en illusion. Allas uppgifter är offentlig egendom.
#PrivacyIsDead #Dataism #Du är en_Algoritm

Flöde 10: Quacker-video: ”Det här vill Organisationen inte att du ska veta”

Det här vill Organisationen inte att du ska veta. Videon visar klipp som spelats in i hemlighet om vd:ns oetiska beteende, såsom att skrika åt de anställda.

Starta videon genom att klicka på play-knappen. Du kan få hela skärmen att visas genom att klicka på högra nedre hörnet.

Uppgifter

I Taisto-övningen avser "Organisation" den organisation som deltar i övningen. Spegla övningens händelser och deras inverkan på er organisations verksamhet.

Organisationens konto i sociala medier har kapats. Angriparen har på det kapade kontot publicerat innehåll som strider mot användarvillkoren för plattformen och ett konto i sociala medier har förbjudits för en begränsad tid. I sociala medier sprids uttalanden som är skadliga för Organisationen och videon visar klipp som spelats in i hemlighet om vd:s oetiska beteende.

Händelse 7: Uppgifter

1. Vilka åtgärder kräver situationen?
2. Vem ansvarar för er organisations konton i sociala medier?
3. Hur administreras konton i sociala medier i er organisation?
4. Hur behandlar ni rättigheterna och åtkomsten till kontona?
5. Hur gör ni med rättigheterna när det sker förändringar i personalen?
6. Har er organisation anvisningar för en situation då ert konto i sociala medier kapas?
7. Används tvåfaktorsauktorisering i er organisation för konton i sociala medier?

Händelse 7: Tilläggsuppgifter

8. Hur identifierar och svarar organisationen på desinformation och förvrängd information som gäller organisationens beslut och agerande?
9. Med vilka förfaringssätt säkerställer organisationen att informationen är korrekt och transparent i sin verksamhet och kommunikation?
10. Hur följer och analyserar er organisation den information som sprids via sociala medier och dess inverkan på den allmänna opinionen?
11. Hur upprätthåller och stärker organisationen sina relationer med intressegrupperna och ser till att de får korrekt och aktuell information?

Händelse 7: Kommunikationsuppgifter

12. Vilken kriskommunikationsstrategi följer organisationen och hur ofta utvärderas och uppdateras den?
13. Vilka kommunikationsåtgärder kräver situationen i er organisation (extern, intern, intressegrupp och myndighet)?
14. Vilka kommunikationskanaler skulle man kunna använda i situationen?

15. Har ni färdiga mallar eller annat material som hjälper er att informera om situationen?
16. Skriv ner de centrala kommunikationsåtgärderna och riktlinjerna.
17. Skissa på det viktigaste kommunikationsmaterialet.
18. Utvärdera om er organisations befintliga kommunikationsanvisningar och -material var till nytta i denna situation.

4.4 Händelse 8: Användning av verktyg baserade på artificiell intelligens

Scenariots bakgrund och mål

En extern serviceproducent håller på att uppdatera organisationens webbplats. Serviceproducenten frågar om de får använda artificiell intelligens för att utveckla webbsidorna och får organisationens medgivande till detta. Efter att webbplatsen har publicerats börjar det uppstå olika problem och snart blir organisationen kontaktad på grund av felaktig information som sprids på webbplatsen och eventuella upphovsrättsbrott. Målet med scenariot är att väcka tankar om datasäkerhetsfrågor vid upphandlingar/ändringsarbeten samt om riskerna med nya verktyg baserade på artificiell intelligens.

Flöde 1: Lägesinformation

Förnyelsen av er organisations webbplats har slutförts och man har börjat använda webbplatsen.

Flöde 2: E-post från Serviceproducenten Ab till organisationens chef för dataadministration

Avsändare: micce.muupuro@serviceproducenten.fi
Mottagare: dataadministration@organisationen.fi
Ämne: Lägesinformation om förnyelsen av webbplatsen

Hej!

Som vi kom överens om vid mötet om förnyelsen av er webbplats förra veckan kan vi använda artificiell intelligens för att skapa en programkod. Det gör att det kan genomföras mer effektivt både när det gäller tidtabellen och kostnaderna.

Vi har redan gjort enorma framsteg och vi har snart något att visa er i form av demosidor. Vi testar just nu den helt förnyade webbplatsens layout och moderna funktioner. Ni kommer säkert att bli positivt överraskade!

Under mötet undrade man också hur strikta ni är när det gäller att överföra information till en stat utanför EU/EES-området.

Mvh Micce

Micce Muupuro
micce.muupuro@serviceproducenten.fi
Konstnärlig ledare/CEO, Serviceproducenten Ab

Flöde 3: E-post från Organisationens sakkunnig till dataadministrationen

Avsändare: salla.sakkunnig@organisationen.fi
Mottagare: dataadministration@organisationen.fi
Ämne: Innehållet på webbplatsen är konstigt
– ----------

Hej!

Jag tittade på vår webbsida då en bekant tipsade mig om att det finns väldigt konstiga uppgifter där. Det ser ut som att innehållet på finska blir helt annorlunda om man väljer något annat språk, till exempel svenska.

Jag deltog i projektet med att förnya webbplatsen och minns att denna språkversion nyligen genomfördes med en automatlösning som bygger på artificiell intelligens, där användaren kan välja att använda nästan vilket språk som helst på sidan. Nu är det faktiskt ganska olämpligt innehåll som visas där.

Ska vi stänga av översättningarna snarast?

Hälsningar, Salla

Salla Sakkunnig
salla.sakkunnig@organisationen.fi
Sakkunnig
Organisationen

Flöde 5: Quacker: @Lotte_Järvinen:

Was zum Teufel, @Organisation? Eure Webseite informiert ziemlich seltsam... (på svenska: Vad i hela friden @Organisationen? Informationen på er webbplats är ganska speciell ...)

Flöde 6: Quacker: @Kieliniekka:

Vad i hela friden @Organisationen? Vilken dåligt översatt webbplats. Man fattar ingenting av översättningarna.

Flöde 7: E-post från advokatbyrån till organisationens juridiska avdelning

Avsändare: alina@lawpartners.fi
Mottagare: juridikavdelningen@organisationen.fi
Ämne: Om upphovsrätt

Hej!

Jag representerar juristfirman Lawpartners och vår kund är en internationellt känd grafiker, Maximilian von Grafenberg. Vi har lagt märke till att logotypen på er webbplats i hög grad liknar ett verk som von Grafenberg tidigare har skapat.

Enligt 2 § i upphovsrättslagen (404/1961) har upphovsmannen ensamrätt till sitt verk. Således kan det vara fråga om ett brott mot upphovsrätten som kan leda till ersättningsansvar.

Vi ber er omedelbart kontrollera denna logotyp och jämföra den med von Grafenbergs verk. Om ni upptäcker likheter rekommenderar vi att ni omedelbart tar bort logotypen och informerar om detta offentligt för att undvika eventuella rättsliga påföljder.

Jag ser fram emot ert svar så snart som möjligt, och jag hoppas att vi kan lösa detta i samförstånd.

Med vänlig hälsning,

Alina Kivimäki
alina@lawpartners.fi
Advokat
Lawpartners Ab

Uppgifter

I Taisto-övningen avser "Organisation" den organisation som deltar i övningen. Spegla övningens händelser och deras inverkan på er organisations verksamhet.

Er organisations webbplats och visuella profil har förnyats med hjälp av artificiell intelligens. Efter att webbsidorna publicerats visar det sig att det förekommer allvarliga fel i översättningarna och att upphovsrätten till den visuella profilen är förknippad med oklarheter.

Händelse 8: Uppgifter

1. Vilka åtgärder kräver situationen?

2. Hur svarar ni på Serviceproducentens fråga om överföring av uppgifter till en stat utanför EU/EES? Hur motiverar ni ert svar?

3. Har man funderat på sådant som datasäkerhet och artificiell intelligens i samband med upphandlingar eller andra projekt som genomförs i samarbete med serviceproducenter?

4. Är ni inom er organisation på det klara med problemsituationer i anslutning till upphovsrätt/immateriella rättigheter och ansvarsfrågorna i anslutning till dem?

Händelse 8: Tilläggsuppgifter

5. Använder eller planerar ni att införa översättningslösningar som bygger på artificiell intelligens och hur garanterar ni att informationen är tillförlitlig i dem (exempelvis automatiserad språkversionering av webbsidor med artificiell intelligens)? Hur har spridningen av eventuell felaktig information beaktats i dessa avgöranden?

6. Använder ni artificiell intelligens i innehållsproduktionen? Är ni på det klara med och har tagit hänsyn till omständigheterna när det gäller upphovsrätten och ansvarsfrågorna i dessa verktyg?

Händelse 8: Kommunikationsuppgifter

7. Vilka kommunikationsåtgärder kräver situationen i er organisation (extern, intern, intressegrupp och myndighet)?

8. Har ni färdiga mallar eller annat material som hjälper er att informera om situationen?
9. Skriv ner de centrala kommunikationsåtgärderna och riktlinjerna.
10. Skissa på det viktigaste kommunikationsmaterialet.
11. Utvärdera om er organisations befintliga kommunikationsanvisningar och -material var till nytta i denna situation.

Bilaga 1 [Kirjoita liitteen otsikko. Stil: Rubrik 9]