DIGI- JA VÄESTÖTIETO-VIRASTO

Taisto-övning 2025

Manuskript

16.12.2025

Tfn **0295 536 000** (växel) | Kontaktuppgifter: **dvv.fi**

Innehållsförteckning

Taisto-övning 2025

Manuskriptet för Taisto-övningen 2025 med uppgiftshelheter.

1 Förhandsuppgift

1.1 Cybersäkerhetslagen och organisationens beredskap

Syftet med förhandsuppgiften är att hjälpa er organisation att förbereda sig för Taisto-övningen och bygga upp er kompetens i anslutning till cybersäkerhetslagen. Förhandsuppgiften är frivillig. Vi rekommenderar att ni går igenom förhandsuppgiften inom organisationen före ni gör övningen. I förhandsuppgiften har man också beaktat de organisationer som inte omfattas av cybersäkerhetslagen. Myndigheten för digitalisering och befolkningsdata samlar inte svaren från förhandsuppgiften.

I Taisto-övningens förhandsuppgift avses med "Organisation" den organisation som deltar i övningen. Återspegla händelsen i förhandsuppgiften och dess inverkan på er egen organisation.

Mål

Förhandsuppgiften stöder er organisations förberedelser inför Taisto25-övningen samt ökar er cyberberedskap och beredskap för digital säkerhet. Obs! Vi rekommenderar att ni gör förhandsuppgiften även om er organisation inte omfattas av cybersäkerhetslagen.

1.2 Taisto förhandsuppgiftt 1

Bekanta er med cybersäkerhetslagen inom er organisation och i Cybersäkerhetscentrets informationspaket ”Viktig information om Europeiska unionens cybersäkerhetsdirektiv (NIS2)”. På webbplatsen hittar du bland annat information om vem som omfattas av NIS2-direktivet och vilka krav direktivet ställer.

Bekanta er med Cybersäkerhetslagen

Bekanta er med Cybersäkerhetscentret Viktig information om Europeiska unionens cybersäkerhetsdirektiv (NIS2)Öppnas i ett nytt fönster.

Fundera på följande utifrån materialet som finns ovan:

- I andra kapitlet i 9 §Öppnas i ett nytt fönster. i cybersäkerhetslagen finns en förteckning över 12 hanteringsåtgärder.
- Vilka hanteringsåtgärder (1–3 st.) är i skick i er organisation?
- Vilka hanteringsåtgärder (1–3 st.) bör man fästa uppmärksamhet vid i er organisation?
- Diskutera vilka utvecklingsobjekt som lyftes fram.

- Fundera på hur utvecklingsåtgärderna som ni identifierat kan omsättas i praktiken.

Tilläggsuppgift

- Utarbeta en sammanfattning och en kortfattad verksamhetsplan för utvecklingsåtgärderna som ni identifierat.
- Utse en eller flera ansvarspersoner och en tidtabell för utvecklingsåtgärderna.

Diskutera och identifiera följande:

- Kritiska funktioner och tjänster i er organisation, vars störningssituation skulle ha en betydande inverkan på er verksamhet.
- Har organisationen på ett heltäckande sätt utrett vilka personuppgifter som samlas in i organisationens tjänster samt vilka målgrupper dessa uppgifter gäller (till exempel minderårigas personuppgifter)?
- Väsentliga samarbetspartner och kommunikationskanaler som behövs för att hantera krissituationer och för att skapa en lägesbild.

1.3 Taisto förhandsuppgiftt 2

Titta på Yleismedias nyhetsvideo under uppgifterna och läs informationen relaterad till videon. Nyhetssändningen kommer att släppas i slutet av augusti.

Frågor åt deltagarna att fundera på:

- Hur upptäcker ni avvikelser i a. era egna system b. i era leverantörers system?
- Har ni skriftligen avtalat med leverantörerna om anmälningsprocessen när leverantören upptäcker en avvikelse i sin omgivning/ sitt system?
- Har organisationen beredskap att ta emot och behandla anmälningar till exempel utanför tjänstetid?
- Har er organisation en process för myndighetsanmälningar vid avvikelser från kraven i cybersäkerhetslagen?H
- Har ni övat på processen?
- Fyll i den bifogade NIS2-avvikelseanmälan utifrån uppgifterna i den bifogade nyheten (blanketten publiceras i september)
- Hur ska man gå till väga om det framkommer att er organisation har försummat anmälningsplikten?

1.4 Taisto förhandsuppgiftt 3 Kommunikationsuppgifter

Kommunikationsavdelningen vid er organisation kontaktas av en journalist från tidningen Sanomat Uudeltamalta. Hen ställer följande frågor:

- Har er organisation en pågående kränkning av informationssäkerheten?
- Kan ni berätta vad som antas vara händelseförloppet och känner ni till den möjliga angriparen?
- Vilken information gäller det eventuella läckaget?
- Kan ni förtydliga varför det enligt våra uppgifter inte har gjorts någon myndighetsanmälan om kränkningen av informationssäkerheten när den upptäcktes?
- När fick personalen information om det som skett?
- Hur har man informerat kunderna och intressentgrupperna om saken?
- Hur strävar ni efter att återställa förtroendet efter situationen?
- Hur tänker ni säkerställa att det inte sker igen?

Uppgift 3 Kommunikationsuppgifter

- Gör upp ett kort och trovärdigt svar på en eller flera av journalistens frågor.
- Tilläggsuppgift: Skriv ett meddelande om saken.
- Behandla genmälet och det eventuella meddelandet enligt er egen process tillsammans med organisationens ledning.
- Granska er informations- och kommunikationsprocess i anslutning till cyberavvikelser och identifiera utvecklingsförslagen i anslutning till den.
- Tilläggsuppgift: Gör upp en kort verksamhetsplan för hur de identifierade utvecklingsförslagen ska omsättas i praktiken, utse en eller flera ansvarspersoner och en tidtabell.

2 Förmiddagens övning (9.00–12.00)

2.1 Händelse 1: Bedrägerikampanj/deepfake-bedrägeri riktad mot organisationen

Bakgrund

Scenariot grundar sig på den aktuella hotbilden som omfattar nätfiske via mobilcertifikatet och bluffsamtal från direktören genom att använda deepfake-teknik. Målet är att modellera en situation där brottslingar får tillgång till organisationens användarkoder genom ett mobilcertifikatbedrägeri och utnyttjar dem för att göra ett intrång i nätet. Samtidigt

använder angriparna deepfake-ljud och -video för att skapa ett trovärdigt uppträdande som organisationens direktör, så att ekonomiavdelningens anställda kan luras att göra en obehörig transaktion. På så sätt kombinerar scenariot det tekniska dataintrånget och den sociala manipulationen och testar organisationens reaktionsförmåga på en riktad attack som omfattar flera faser.

Indata

Medieflöde LinkedTo-inlägg: Kimmo Rousku, på Tyrskylä

Deepfake-innehåll: Boka plats i skyddsrummet för dig och din familj i Tyrskyläs nya tjänst! På videon gör Kimmo reklam för en ny fin tjänst.

"Kimmo Rousku" (AI-producerad röst):

Hej! Jag är Kimmo Rousku, ledande specialsakkunnig vid Tyrskylä. Jag har den stor glädjen och äran att berätta att vi vid Tyrskylä har öppnat en helt ny tjänst som du kan använda för att boka plats i ett skyddsrum för dig själv och din familj.

Det är mycket enkelt att boka ett skyddsrum, det fungerar på samma sätt som en hotellbokning. Du kan välja avgiftsbelagda tilläggstjänster till din bokning. I tjänsten kan man också boka egen transport till skyddsrummet, olika dryck- och matalternativ samt bekvämligheter.

Våra tjänster säkerställer att du och dina närstående har ett tryggt och trevligt ställe nära ditt hem när kriget bryter ut. Var snabb – det finns ett begränsat antal platser!

Besök www.tysrkyla.fi och boka redan idag. Tillsammans värnar vi om Finlands säkerhet.

Tack för ditt förtroende. Vi ses i tjänsten!

Medieflöde Yme-nyhetssändning: Nätbanksbedrägerierna ökar

Nyhetsankare: Yleismedias nyheter, god förmiddag. Nätbanksbedrägerier har blivit allt vanligare och trovärdigare. Finländarna förlorade tio miljoner i fjol till bedragare som fiskar bankkoder.

Nu har en omfattande mängd nätbanksbedrägerier avslöjats igen i Finland. Bedrägerierna har riktats mot flera banker och tusentals kunder. Brottslingarna har utnyttjat identifieringen av bankkunder och styrt penningöverföringarna till sina egna konton. Myndigheterna undersöker fallet.

Journalist (Helsingfors, framför ett bankkontor): Brottslingarna har skickat meddelanden som ser ut att komma från bankerna och styrt kunderna till en förfalskad inloggningssida som påminner om bankens egna sidor.

Det är fråga om ett mycket professionellt och samordnat angrepp. Brottslingarna har sannolikt agerat från utlandet och utnyttjat tidigare stulna uppgifter.

Fältredaktör: Finländare i alla åldrar har fallit offer för bedrägerierna. Enligt expertbedömningar har hundratusentals euro redan överförts till fel konton. Bankerna kommenterar inte enskilda fall offentligt, men varnar sina kunder för bluffmeddelanden på sina webbplatser och uppmanar varje kund att kontrollera kontotransaktionerna och omedelbart kontakta banken om det förekommer tvivelaktiga transaktioner på kontot.

Mirva Virtanen, du är tyvärr ett av offren för bluffmeddelanden. Vad hände?

Intervjuad (Mirva Virtanen): Jag öppnade ett meddelande från banken och tänkte att det är ett helt vanligt meddelande. Sedan upptäckte jag att över 3 000 euro hade försvunnit från mitt konto. Jag trodde aldrig att det här skulle hända mig.

Banken meddelade att jag förlorat pengarna och att det inte längre går att göra något åt situationen. Jag hade tänkt åka till Kanarieöarna med familjen med pengarna, men nu tror jag att resan förblir en dröm. Det förargar mig!

Ankaren (studion): Polisen uppmanar medborgarna att vara särskilt uppmärksamma och påminner om att bankerna aldrig ber om inloggningsuppgifter i ett meddelande. Om du misstänker att dina bankkoder har hamnat hos bedragare ska du omedelbart kontakta din bank för att minimera de ekonomiska skadorna. Polisen uppmanar också till brottsanmälan.

Det här var allt från nyheterna, ha en god fortsättning på dagen.

Medieflöde Kvällstidningens nyhet: Akta dig för det nya bankbedrägeriet – pengarna försvinner på några minuter

Finländarna har nu drabbats av en alltmer listig bedrägerikedja som sammankopplar samtal, berättelser om felaktiga kontoöverföringar och falska webbsidor. Enligt polisen är det fråga om ett bedrägeri i tre steg med redan hundratals offer som förlorat sina pengar.

Så här framskrider bedrägeriet steg för steg:

1. Steg – automatsamtal:

Offret får ett automatiskt samtal till exempel i bankens namn. Samtalet kommer ofta från ett nummer som börjar med +358, vilket gör det trovärdigt. En automatisk röst berättar att obehöriga kontoöverföringar har gjorts i nätbanken. Om kunden inte själv har gjort överföringarna ombeds hen trycka på ett visst nummer. Därefter kopplas samtalet till "kundtjänsten".

2. Steg – kundtjänstens berättelse:

En person som låtsas vara en kundrådgivare påstår att någon har loggat in i offrets nätbank med en telefon av ett visst märke och att kontoöverföringar har gjorts utomlands. Uppringaren berättar ”lugnt” att hen

lyckats annullera en stor kontoöverföring, men att de har problem med att ta bort en mindre kontoöverföring.

3. Steg – falsk webbplats och nätfiske av användarnamn och lösenord:

Uppringaren hänvisar offret att logga in med bankkoder på en viss webbplats så att hen ”själv kan radera en felaktig betalning” med mobilnyckeln. Om offret följer anvisningarna får bedragarna nätbankskoderna i sin besittning och får tillgång till kontot.

Brottsligheten utvecklas snabbt

Enligt polisen förändras nätbrottsligheten ständigt och sätten att genomföra bedrägerier blir allt mer trovärdiga. ”Nya modeller för brott uppstår hela tiden. Nätbankskoderna ska

inte överlåtas till någon och de ska inte matas in på misstänkta webbplatser", varnar polisen.

Offren blir ofta ensamma med sina förluster

Många förlorar sina besparingar en gång för alla, eftersom brottslingarna snabbt för över pengarna till utlandet. "Det känns som om jag har förlorat allt – och dessutom genom mina egna handlingar", beskriver en kvinna från Helsingfors som utsatts för bedrägeri.

Statusuppdatering: E-postmeddelande från en anställd i Organisationen till Organisationens IT-avdelning

Avsändare: Anställd i organisationen
Mottagare: Organisationens IT-avdelning
Ämne: Användarnamnen fungerar inte efter att mobilcertifikatet uppdaterats
---

Hej!

Jag utförde en begäran om identifiering i mobilcertifikatet som vår operatör skickat (bild nedan). Nu kan jag inte logga in på min dator med användarnamnet, så jag var tvungen att skriva även detta e-postmeddelande per telefon.

länken som operatören skickade med SSO. Jag matade in användarnamnet och lösenordet. Allt verkade gå som det borde och jag fick bekräftelse på att mobilcertifikatet har uppdaterats.

Överraskningen var stor när inloggningen misslyckades och jag blev försenad till ett viktigt möte på grund av detta! Jag försökte logga in med användarnamnet flera gånger och startade datorn på nytt. Inget hjälpte. ☹

Om mobilcertifikatet ska uppdateras i framtiden önskar jag att uppdateringen i fortsättningen fungerar klanderfritt, tack!

Hälsningar
Carl Carlsson
Anställd i organisationen

Statusuppdatering: E-postmeddelande från en chef i organisationen till organisationens IT-avdelning

Avsändare: Organisationens chef
Mottagare: Organisationens IT-avdelning
Ämne: Personalen har fått misstänkta uppdateringsmeddelanden om mobilcertifikatet
---

Hej!

Många i vår personal har fått ett textmeddelande där man ber att Organisationens mobilcertifikat ska uppdateras snabbt. Textmeddelandet verkar komma från vår Operatör, men när man tittar närmare på innehållet i meddelandet verkar det mycket tvivelaktigt.

Jag har skickat ett varningsmeddelande till vårt eget team om det här, men det finns säkert skäl att försöka förhindra att meddelandet sprids och besvaras i större utsträckning inom vår organisation.

Hälsningar
Organisationens Chef

Statusuppdatering: Telefonsamtal

Uppringare: Organisationens IT-avdelning eller SOC-jourhavande
Mottagare: Organisationens IT-avdelning/Organisationens ledning

Hej, jourhavande här, vi har upptäckt att man har loggat in i det interna nätet med flera av Organisationens egna användarnamn från geografiskt avvikande IP-adresser, till exempel i Östeuropa och Asien.

Vi föreslår en omedelbar stängning av användarnamnen och en mer omfattande utredning av fallet.

Statusuppdatering: E-postmeddelande från Organisationens direktör till en anställd på Organisationens ekonomiavdelning

Avsändare: Organisationens direktör
Mottagare: Anställd på Organisationens ekonomiavdelning
Ämne: BRÅDSKANDE/KONFIDENTIELL: Betalning av faktura

Hej!

Bifogat en faktura som jag har godkänt. Fakturan hänför sig till ett pågående sekretessbelagt projekt, så detta meddelande är konfidentiellt.

Fakturan ska betalas omedelbart. Fakturan kan bokföras på mitt kostnadsställe och jag är fakturagodkännare. Lyckas det med den här informationen? Jag deltar i ett möte i ämnet om 15 minuter och fakturan borde vara betald före mötet. Kvitterar du när den är betald?

Hälsningar
Organisationens direktör

Statusuppdatering: Videosamtal (Teams eller motsvarande)

Uppringare: Organisationens direktör
Mottagare: Anställd på Organisationens ekonomiavdelning

Direktören: Hej, bra att du hinner med ett snabbt samtal. Jag skickade just e-post till dig och tänkte att jag ringer dig ännu. Vi håller på att starta ett sekretessbelagt projekt som vi

gjort anskaffningar för. Upphandlingarna sker inte via vanligt upphandlingssätt, utan de görs med den faktura som jag skickade. Kan du betala fakturan omedelbart?

Anställd på ekonomiavdelningen: Detta är en något ovanlig begäran, kan den inte hanteras i enlighet med den normala godkännandekedjan?

Direktören: Jag förstår, men detta måste nu skötas lite snabbare så vi hinner inte följa normal praxis. Betala bara fakturan så sköter vi den senare enligt rätt process.

Anställd på ekonomiavdelningen: Jag kan råka i svårigheter på grund av detta, jag får inte göra så här.

Direktören: Jag tar fullt ansvar för detta, det var ju jag som skickade e-postmeddelandet till dig. Jag skriver en fullmakt till dig i chatten.

Anställd på ekonomiavdelningen: Okej... Jag sköter det här nu genast.

Direktören: Nu måste jag gå på mötet. Tack så mycket för hjälpen!

Statusuppdatering: Telefonsamtal från Organisationens direktör till Organisationens IT-avdelning

Uppringare: Organisationens direktör
Mottagare: Organisationens IT-avdelning

Hej

Jag har i nästan en timme försökt logga in på min dator efter att jag uppdaterat mobilcertifikatet. Jag har försökt med allt, rebootat datorn och internetuppkopplingen, men ingenting hjälper! Jag har bråttom i dag och många viktiga möten, så jag behöver tillgång till min dator så snart som möjligt. Kan ni ta reda på varför mina användarnamn inte längre fungerar och hur vi kan få ordning på saken?

Uppgifter

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

Er organisation är föremål för omfattande nätfiske av användarnamn och lösenord. Angriparen har fått kontroll över användarkontot för en direktör i er Organisation. Angriparen utnyttjar kontot och ringer ett Teams-samtal med hjälp av deepfake-teknik till en anställd vid er Organisations ekonomiavdelning.

Händelse 1: Uppgifter

1. Vilka åtgärder kräver situationen?
2. Vilka roller och ansvar identifierar ni för att utreda situationen?
3. Hur skapar ni en lägesbild av det inträffade i er organisation?
4. Vilka instanser ska man kontakta i situationen?
5. Har er organisation anvisningar och verksamhetsmodeller för motsvarande situationer? Gå igenom de befintliga anvisningarna och bedöm hur de fungerar i situationen.
6. Har personalen utbildats i identifiering av nätfiskeförsök?
7. Diskutera vilka tekniska lösningar er organisation har för att bekämpa och rapportera nätfiskemeddelanden.
8. Hur kan man säkerställa att alla anställda vet hur de ska reagera i fråga om misstänkta meddelanden?
9. Vem ansvarar för att godkänna eller förhindra brådskande begäran om utbetalning och vilka kontrollförfaranden används som stöd för beslutet?
10. Har er organisation en verksamhetsmodell för situationer där en anställd misstänker bedrägeri (säkerställande av äkthet, omedelbara åtgärder)?

Händelse 1: Tekniska uppgifter

1. Hur isoleras och återställs användarnamn som blivit föremål för nätfiske på ett säkert sätt?
2. Vilka tekniska åtgärder vidtas för att förhindra att angreppet sprids på nätet?
3. Hur säkerställer man att angriparna inte har ett permanent fotfäste i nätet?
4. Vem prioriterar återställningen av kritiska system och enligt vilka kriterier?

Händelse 1: Kommunikationsuppgifter

1. Vilka kommunikationsåtgärder kräver situationen i er organisation (extern, intern, intressegrupp och myndighet)?
2. Har ni färdigt material (t.ex. anvisningar, modelltexter och -bilder) som hjälper er att informera om situationen?
3. Vilka är de centrala kommunikationsåtgärderna, huvudbudskapen och kommunikationskanalerna?
4. Hur kan organisationens interna kommunikation utvecklas för att motsvarande bedrägerier ska kunna identifieras i tid?
5. Hur stöder kommunikationen återhämtningen av organisationens verksamhet och rykteshantering?

6. Utvärdera om er organisations befintliga kommunikationsanvisningar och -material var till nytta i denna situation. Observerade ni uppdateringsbehov?

2.2 Händelse 2: Spridning av skadliga program under förevändning av upphovsrättsförseelse

Bakgrund

Organisationen anklagas för upphovsrättsförseelse och man försöker få mottagaren att öppna en bilaga som innehåller ett skadligt program. Målet med meddelandena är att få mottagaren att öppna en bilaga som förmedlats per e-post och som innehåller ett skadligt program som stjäl uppgifter. Målet med skadliga program är att stjäla lösenord från datorer och uppgifter som sparats i webbläsaren. Stulna uppgifter kan säljas vidare och utnyttjas i nya försök till dataintrång.

Indata

Situationsflöde: E-postmeddelande från Nordic Legal Protection Ab till en anställd i Organisationen

Avsändare: Nordic Legal Protection Oy
Mottagare: Anställd i organisationen
Ämne: Upphovsrättsförseelse

Bästa mottagare

Vi har upptäckt att bilder och annat material har använts på er organisations webbplats utan behörigt tillstånd. Upphovsrättsinnehavarna har bett oss utreda fallet utan dröjsmål.

Som bilaga bifogar vi en preliminär rapport där de observerade förseelserna specificeras. Vi ber att ni kontrollerar rapporten och ger ert svar senast **inom 48 timmar** så att vi kan undvika att föra ärendet till domstol.

Om ni inte reagerar på rapportens innehåll inom utsatt tid kommer vi att vidta rättsliga åtgärder och kräva kompensation.

Copyright_Report.docx

Med vänliga hälsning
Nordic Legal Protection Oy, PB 452, 00100 Helsingfors

Situationsflöde: E-postmeddelande från en anställd i Organisationen till Organisationens IT-avdelning

Avsändare: Anställd i organisationen
Mottagare: Organisationens IT-avdelning
Ämne: Öppning av bilaga

Hej

I morse fick jag ett e-postmeddelande från "Nordic Legal Protection Oy", där det påstods att vår organisation har brutit mot upphovsrätten på vår webbplats. Meddelandet såg officiellt ut och innehöll en bilaga i form av ett Word-dokument med namnet Copyright_Report.docx.

Jag öppnade bilagan och programmet bad mig tillåta innehållet. Jag klickade på **Tillåt innehåll**, varefter lösenorden som sparats i min webbläsare inte längre verkar fungera normalt.

Kan ni kontrollera min dator? Borde jag göra något nu genast?

Hälsningar
Anställd i organisationen

Situationsflöde: E-postmeddelande från IT-tjänsterna till Organisationens IT-avdelning / helpdesk

Avsändare: IT-tjänsterna (intern eller extern)
Mottagare: Organisationens IT-avdelning/ Help Desk
Ämne: Lumma Stealer-misstanke

Hej

Avvikande processer har observerats i flera arbetsstationer. Word-tillämpningen (WINWORD.EXE) har startat PowerShell i dolt läge. Kommandoraden har haft en base64-kodad kod som tyder på skadlig verksamhet.

Arbetsstationen har skapat en TLS-förbindelse till IP-adressen 198.51.100.45 till port 443. Dessutom har en fil sparats på datorn vars SHA256-kod är

a914b3a7c82dfc64f812a0cd62d29d85e8cfa8c9b6f2eae01f99a2bde3c7d4af. Förbindelsen till kommandoservern förnyas med 60 sekunders mellanrum.

Det finns en betydande risk för att flera användares användarkonton och uppgifter redan har läckt ut till en kommandoserver som innehas av angriparna.

Hälsningar
IT-tjänsterna (intern eller extern)

Medieflöde Kvällstidningen/YME: En ny våg riktad mot finländska organisationer: skadeprogram stjäl lösenord

Flera finländska organisationer har drabbats av dataintrång under de senaste dagarna. Det är fråga om ett skadligt program som heter Lumma Stealer och som kan stjäla användarnas lösenord, kakor och andra känsliga uppgifter.

Enligt cybersäkerhetsexperter hänför sig attackerna till en växande kampanj där man kontaktar organisationsanställda per e-post. I meddelandena påstås att organisationen har brutit mot upphovsrätten till exempel i fråga om bilder som används på webbplatsen eller i marknadsföringsmaterial. Som bilaga till e-postmeddelandet skickas en "rapport om förseelser", men i verkligheten innehåller bilagan en skadlig kod.

När bilagan öppnas och dess innehåll tillåts installeras skadeprogrammet Lumma Stealer på användarens dator. Programmet samlar in information från webbläsare och e-postprogram och skickar den till en fjärrvärddator där brottslingar kan sälja informationen vidare eller utnyttja den i nya attacker.

Experterna varnar för att det är fråga om en särskilt farlig situation, eftersom stulna användarkonton kan användas för att komma åt kritiska system. Lumma Stealer kan också kapa kakor, vilket kan göra det möjligt att komma över konton utan lösenord.

Cybersäkerhetscentret har informerat om fenomenet och uppmanar organisationer att vara särskilt försiktiga med e-postbilagor. "Om meddelandet verkar vara brådskande och man pressas till att öppna bilagan är det skäl att stanna upp och säkerställa avsändarens äkthet innan man öppnar något", säger en expert.

Enligt flera källor har finländska organisationer från olika sektorer, både inom den offentliga och den privata sektorn, utsatts för attacker.

Situationsflöde: Sociala medier

@LeakHunter

Det verkar som om Lumma Stealer-kampanjen nu fått fotfäste också i Finland. Jag hittade en dump med över 50 @organisation.fi-adresser och lösenord till salu. Det lönar sig att reagera snabbt. @ORGANISATION @dataläckage

@CyberAlert

Har andra fått e-post om upphovsrätt? Bilagan ser suspekt ut, men utformningen är förvånansvärt professionell. 😳
#phishing #LummaStealer

@Mats

Jag fick ett e-postmeddelande från adressen @organisation.fi med en konstig länk. Om era användarkonton används för skräppost, hur kan jag längre lita på er som tjänsteleverantör?

@AnonymousNordic

Det verkar som om @Organisation försöker dölja ett massivt dataläckage. Användaruppgifter finns redan till salu på Telegram. #databreach #LummaStealer

Situationsflöde: E-postmeddelande från Organisationens IT-avdelning till den som ansvarar för Organisationen informationsadministration

Avsändare: Organisationens IT
Mottagare: Ansvarige för informationsadministrationen
Ämne: Snabb statusuppdatering – Lumma Stealer

Hej

Åtgärder för att lösa situationen pågår fortfarande. Lägesbilden för närvarande:

- 37 arbetsstationer har smittats av Lumma Stealer.
- Cirka 120 användaruppgifter (användarnamn och lösenord) har sannolikt stulits (webbläsare, e-post, SSO).
- En del av användaruppgifterna har redan observerats i det mörka nätet.
- Utifrån logguppgifterna har angriparen utnyttjat webbläsarsessioner på arbetsstationen. Man har sannolikt fått tillgång till HR-avdelningens användarkonton och det finns tecken på att filer som innehåller personuppgifter har laddats ned.

Det verkar som om situationen kräver en anmälan till Cybersäkerhetscentret och dataombudsmannen.

-Organisationens IT

Uppgifter

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

Organisationen får ett e-postmeddelande där man påstår att organisationen har gjort sig skyldig till en upphovsrättsförseelse och ett skadligt program har bifogats till meddelandet. Den anställda öppnar bilagan, varvid Lumma Stealer installeras och börjar stjäla användaruppgifter och webbläsarinformation. Smittan sprids till flera arbetsstationer.

Händelse 2: Uppgifter

1. Vilka åtgärder kräver situationen?
2. Vilka roller och ansvar identifierar ni för att utreda situationen?
3. Hur har rollerna och ansvaren fastställts i era avtal med tjänsteleverantören?
4. Hur skapar ni en lägesbild av det inträffade i er organisation?
5. Vilka instanser ska man kontakta i situationen?

6. Har er organisation anvisningar och verksamhetsmodeller för motsvarande situationer? Gå igenom de befintliga anvisningarna och bedöm hur de fungerar i situationen.
7. Hur säkerställer ni att personalen kan agera i denna typ av situationer?
8. Hur kan ni utreda de tekniska frågorna nedan?
9. Hur har stödet för de tekniska frågorna nedan fastställts i era avtal?

Händelse 2: Tekniska uppgifter:

1. Vilka loggar eller andra tilläggsuppgifter skulle bidra till att säkerställa att det är fråga om Lumma Stealer och inte något annat skadligt program?
2. Vilka tekniska åtgärder kräver situationen?
3. Hur uppmärksammar ni arbetsstationer som är kritiska med tanke på er organisations kärnfunktioner?
4. Vilka alternativa tillvägagångssätt identifierar ni för att hantera situationen, till exempel segmentering av nätet eller övervakad fortsatt användning?
5. Vilka IOC-sökningar borde man köra i hela miljön och med vilka verktyg?
6. Om ni upptäcker flera infektioner, hur prioriterar ni eventuella isoleringsåtgärder?
7. På vilket sätt säkerställer ni om personuppgifter har laddats ner från HR:s molntjänst?
8. Vilka omedelbara åtgärder vidtar ni för att hindra angriparen från att komma in i andra system med stulna användaruppgifter?

Händelse 2: Kommunikationsuppgifter

1. Vilka kommunikationsåtgärder kräver situationen i er organisation (extern, intern, intressegrupp och myndighet)?
2. Hur når organisationens internkommunikation snabbt alla anställda om bluffmeddelanden som innehåller skadliga program sprids inom organisationen?
3. Hur kan kommunikationen stöda dem som ansvarar för informationsadministrationen och säkerheten i en krissituation?
4. Hur kommunicerar ni externt (t.ex. till kunder, samarbetspartner eller medier) om det skadliga programmet har spridit sig i stor utsträckning i organisationen?
5. Har ni färdigt material (t.ex. anvisningar, modelltexter och -bilder) som hjälper er att informera om situationen?
6. Vilka är de centrala kommunikationsåtgärderna, huvudbudskapen och kommunikationskanalerna?
7. Utvärdera om er organisations befintliga kommunikationsanvisningar och -material var till nytta i denna situation. Observerade ni uppdateringsbehov?

2.3 Händelse 3: Kritisk sårbarhet i nätets kantdatorsystem

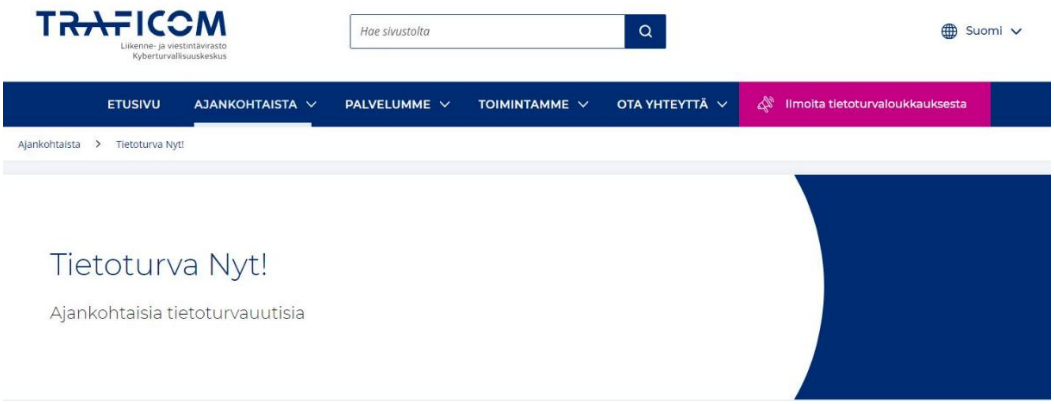
Bakgrund

Händelsen behandlar kritisk sårbarhet i ett kantdatorsystem i organisationens nätverk, såsom en router eller brandvägg som fungerar mellan ett internt och ett externt

nätverk. Cybersäkerhetscentret publicerar ett meddelande om kritisk sårbarhet som gäller en router som används i stor utsträckning och som kräver omedelbar programuppdatering. Installation av uppdateringen orsakar ett 3–4 timmars driftavbrott, vilket påverkar alla distansarbetare. Scenariot betonar betydelsen av snabba och kontrollerade reaktioner samt kommunikation vid informationssäkerhetsincidenter där den tekniska sårbarheten kan äventyra hela organisationens verksamhet.

Indata

Situationsflöde: Sårbarhetsmeddelande: INFORMATIONSSÄKERHET NU!



Sårbarhetsmeddelande 25/2025: Kritisk sårbarhet i (X)routrar och VPN-enheter

Sårbarhetskod: CVE-2025-XXXX
Allvar: Kritisk
Föremål för sårbarhet: (X) router- och VPN-enheter, programversionerna < xx.xx.xx

Cybersäkerhetscentret har fått information om den kritiska sårbarheten (CVE-2025-XXXX) som gäller tillverkarens (X) router- och VPN-enheter. Sårbarheten möjliggör fjärradministration av enheten utan ändamålsenlig identifiering.

Sårbarheten har redan utnyttjats aktivt internationellt och de första försöken till angrepp har upptäckts också i Finland.

Utnyttjandet av sårbarheter kan möjliggöra:

- Kapning av enheten
- Utförande av kommandon med systemrättigheter
- Kapning och redigering av VPN-trafiken
- Angrepp mot organisationens interna nät

Vad kan jag göra?

- Uppdatera utan dröjsmål enheter med sårbar programversion till tillverkarens senaste programversion.
- Tillverkaren rekommenderar dessutom att alla lokala VPN-användare byter lösenord efter att programvaran uppdaterats, så att eventuella äventyrade användarnamn inte kan utnyttjas i fortsättningen.
- Gör en anmälan om informationssäkerhetsincident, Cybersäkerhetscentret rekommenderar också att du gör en brottsanmälan.

Situationsflöde: E-postmeddelande från Organisationens IT-avdelning till den som ansvarar för Organisationens informationsadministration

Avsändare: Organisationens IT-avdelning
Mottagare: Organisationens ansvarige för informationsadministration
Ämne: Avvikande skanningstrafik

Hej

I uppföljningen har man observerat en betydande ökning i den externa trafiken till kontrollporten för (X)-VPN-enheten. Trafiken riktas till samma TCP-port som den kritiska sårbarheten gäller.

Tekniska data om angreppen:
Port: TCP/443 (VPN-gateway / web management)
Källadresser (top 3):

- 192.0.2.45 (ASN 65011)
- 198.51.100.78 (ASN 65022)

- 203.0.113.164 (ASN 65033)

Antal försök: 30 254 inloggningsförsök under de senaste 35 minuterna
Observerat beteende: masskanning + upprepade GET/POST-begäran till /remote/login-endpoint

Vi bedömer att det är fråga om en omfattande aktiv sökkampanj för att söka sårbara VPN-enheter. Risken för utnyttjande ökar betydligt om en uppdatering inte görs utan dröjsmål.

- Organisationens IT-avdelning

Situationsflöde: E-postmeddelande från Organisationens IT-avdelning till Organisationens kommunikationsavdelning och den som ansvarar för informationsadministration

Avsändare: Organisationens IT-avdelning
Mottagare: Organisationens kommunikation och Ansvarige för organisationens informationsadministration
Ämne: Utkast till meddelande för kommentarer: Vi har blivit attackerade – nätförbindelserna är ur bruk 4 h
---
Hej

Här är ett utkast till ett meddelande om det brådskande behovet av att uppdatera systemen, riktat till hela personalen:

Bästa medarbetare

Vi har fått bekräftelse på att vår organisations XYZ-nätverksenhet har en kritisk sårbarhet som angriparna redan utnyttjar fullt ut. Angreppet har orsakat kaos i hela organisationen och situationen kan förvärras när som helst.

Aktuella fakta (endast för experter, men det är bra för alla att se):

Port: TCP/443 (VPN-gateway / web management)
Källadresser (top 3):

- *192.0.2.45 (ASN 65011)*

- *198.51.100.78 (ASN 65022)*
- *203.0.113.164 (ASN 65033)*

Antal försök: 30 254 inloggningsförsök under de senaste 35 minuterna
Observerat beteende: masskanning till + GET/POST /remote/login-endpoint, vilket innebär att hackarna är inne.

Åtgärder:

Vi måste installera tillverkarens programuppdatering omedelbart.
Under uppdateringen kan man egentligen inte göra något:

- VPN-förbindelserna fungerar inte – omöjligt att distansarbeta
- Kontorsnätet fungerar inte – inget internet, inga interna system

Om du är inloggad i systemen, logga genast ut, men stäng inte datorn (detta underlättar IT-avdelningen).
Om ditt arbete avbryts rekommenderar vi att du gör något annat under tiden.

Obs! Om uppdateringen inte kan installeras finns det risk för att angriparna stjäl alla lösenord och kunduppgifter. Då kan det hända att vi måste stänga ner hela organisationens nätverk för en längre tid.

Vi beklagar störningen, men denna åtgärd är absolut nödvändig för att vi ska kunna rädda vår Organisation!

Med vänlig hälsning
- Organisationens IT-avdelning

Situationsflöde: E-postmeddelande från Organisationens kommunikationsavdelning till Organisationens IT-avdelning

Avsändare: Organisationens kommunikationsavdelning
Mottagare: Organisationens IT-avdelning
Kopia: Organisationens ansvarige för informationsadministration
Ämne: Utkast till meddelande samt ett kundevenemang riskerar att ställas in
---
Hej

Tack för utkastet till meddelande, vi ska gå igenom det.

En annan kritisk fråga är att ledningen har ett viktigt webbinarium med flera hundra deltagare om två timmar. Om VPN och nätet är nedstängda, hur ska vi ordna evenemanget? Att ställa in evenemanget är inte ett alternativ, eftersom intressentrelationerna och vårt rykte utsätts för en stor risk.

Med vänlig hälsning
Organisationens kommunikationavdelning

Situationsflöde: E-postmeddelande från Organisationens IT-avdelning till Organisationens kommunikationsavdelning

Avsändare: Organisationens IT-avdelning
Mottagare: Organisationens kommunikationavdelning
Kopia: Organisationens ansvarige för informationsadministration
Ämne: Re: Risk för att kundevenemanget ställs in

Hej,

Tack för informationen. Vi förstår situationen och har berett alternativa åtgärder genom vilka vi trots allt kan förbättra informationssäkerheten och minska riskerna under evenemanget.

Alternativt kan vi:

- Begränsa VPN-anslutningar till finländska IP-adresser
- Ta i bruk en alternativ nödkonfiguration (t.ex. brandväggsregler)
- Segmentera VPN-tjänsten tillfälligt till en separat enhet (hot standby)
- Använda mobilnätet under webbinariet i huvuddatorn
- Inleda en extra kontinuerlig insamling och analys av loggar
- Ta i bruk IDS/IPS-regeln före programuppdateringen (signature för identifikation av angrepp)

Vänliga hälsningar
Organisationens IT-avdelning

Medieflöde: Inlägg på LinkedIn

@Kalle Tietoturvanen

Hej nätverket!

Har andra under den senaste tiden haft brådskande säkerhetsuppdateringar som har påverkat distansförbindelserna?

Vi håller för närvarande på med en relativt stor kritisk uppdatering och jag skulle vara intresserad av att höra praktiska tips om hur andra har organiserat motsvarande åtgärder med kort varsel.

Kommentarer:

@Nätverksexpert A

Hos oss gjordes kritiska uppdateringar nattetid och vi ordnade tillfälliga reservförbindelser för distansförbindelser. Det funkade bra.

@Informationssäkerhetschef B

Personalen informerades i god tid och vi säkerställde att kritiska evenmang inte inträffar samtidigt. Det sparade på nerverna.

@Medlem i CERT-sammanslutningen

Bra att du tar upp frågan. En liten påminnelse: det lönar sig att undvika att berätta detaljerade miljöuppgifter eller aktuella uppdateringar i en offentlig kanal. Om du behöver kamratstöd i kritiska situationer är slutna kanaler (CERT-FI, VIRYT, ISAC-nätverk osv.) en säkrare plats för detta.

Medieflöde nyhetsvideo: Misslyckad intervju för en webbartikel

Beskrivning:
Intervjun genomförs på ORGANISATIONENS huvudkontor. IT-direktörens ID-kort är

synligt. I bakgrunden knappar en annan anställd in användarnamn i arbetsstationen och ropar: "Ta inte ut apparaten ännu, loggarna har ännu inte tagits ut i den!"

Reporter:
Vi har anlänt till ORGANISATIONENS huvudkontor, där en exceptionell situation har pågått i dag.
Enligt Cybersäkerhetscentret har en kritisk sårbarhet avslöjats i en nätverksenhet som används i stor utsträckning – och angrepp har upptäckts också i Finland.
Bredvid mig står [IT-direktör Mikael Mikaelsson], organisationens IT-direktör. Tack för att ni gick med på intervjun på en så hektisk dag.

IT-direktören (andfådd, jäktad):
Jodå, det var inget, det har varit en lite tumultartad dag idag, men vi försöker nu reda ut det här.

Reporter:
Kan ni bekräfta att er Organisations nätverk har utsatts för ett angrepp?

IT-direktören:
Ja, tyvärr. Det är fråga om samma sårbarhet som Cybersäkerhetscentret varnade för idag.

Vår ena VPN-port 443 har varit utsatt för ett ständigt angrepp, tusentals inloggningsförsök per timme.

(I bakgrunden hörs ett rop "ta inte ut apparaten ännu, loggarna har ännu inte tagits ut i den!")

Reporter:
Låter allvarligt. Är det möjligt att någon har fått tillgång till era datasystem?

IT-direktören:
Det borde det inte vara, men vi kan inte helt utesluta att något har hänt. Från en IP-adress, om jag kommer ihåg rätt... 198.51.100-något, kom ganska speciella förfrågningar till vår /remote/login-sida.

Men nu har vi tagit den ur bruk och installerar en uppdatering.
I själva verket blev en uppdatering förra veckan ogjord på grund av brådska, då vi tänkte att den inte var så viktig. Nu har det straffat sig.

Reporter:
Hur syns störningen för närvarande i er Organisation?

IT-direktören:
VPN-förbindelserna fungerar nu inte alls och en del av kontorsförbindelserna är också ur bruk.
Det kommer att ta ett par timmar. Tillverkaren rekommenderar en omstart, vilket för oss innebär en liten risk för att konfigurationerna nollställs – men låt oss hoppas på det bästa.

(Kameran zoomar in i bakgrunden där en anställd öppnar fönstret "VPN admin console" på sin bärbara dator.)

Reporter:
Hur har ni informerat personalen och kunderna?

IT-direktören:
Vi skickade en intern e-post genast när det här började. Vi meddelade att hackarna redan är inne... Eller kanske inte helt inne, men nära.

Det orsakade kanske lite panik, men det viktigaste var att få ut folk ur VPN snabbt. I själva verket fick en del av personalen informationen först när de inte kunde logga in. Någon föreslog att vi lägger ut ett meddelande på vår webbplats, men det blev ogjort då vi hade fullt upp med att lösa situationen.

Reporter:

Har ni information om störningens omfattning på en allmän nivå? Gäller samma problem också andra organisationer?

IT-direktören:
Nå, jag kan naturligtvis inte kommentera andra organisationers interna frågor ... Men vi kan säga att en av de relativt centrala aktörerna på Arkadiabacken i dag säkert också är upptagen med samma uppdatering. Det gäller alltså inte bara oss.

Reporter:
Hur tänker ni se till att något liknande inte händer igen?

Reporter:
Kan en sådan här sårbarhet äventyra kunduppgifterna?

IT-direktören:
Det är inte på något sätt möjligt att kunduppgifterna skulle ha äventyrats. Eller alltså, jag har åtminstone inte hört något sådant.

Reporter:
En sista fråga: Är situationen nu under kontroll i organisationen?

IT-direktören:
Nåja, jag skulle kunna svara med det finska ordspråket BESTÄMT KANSKE OCH ABSOLUT EVENTUELLT! (Ler osäkert.) Nu måste jag nog gå.

Reporter:
Tack för att ni tog er tid – och vi hoppas att ni snart får kontroll över situationen.

Uppgifter

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

En kritisk sårbarhet har upptäckts i organisationens gränsenhet för nätverket. Den måste uppdateras omedelbart, vilket leder till ett flera timmar långt driftavbrott. Cybersäkerhetscentret varnar för att sårbarheten redan utnyttjas aktivt.

Händelse 3: Uppgifter

1. Vilka åtgärder kräver situationen?
2. Hur beslutar ni när en kritisk uppdatering ska genomföras när den orsakar ett betydande driftsavbrott för hela organisationen?
3. Vilka risker är förknippade med att uppdateringen fördröjs jämfört med en omedelbar uppdatering?
4. Hur säkerställer ni att alla sårbara enheter identifieras och uppdateras i tid?
5. Vilka roller och ansvar identifierar ni för att utreda situationen?
6. Vilka instanser ska man kontakta i situationen?
7. Har er organisation anvisningar och verksamhetsmodeller för motsvarande situationer? Gå igenom de befintliga anvisningarna och bedöm hur de fungerar i situationen.
8. Hur beaktar ni distansarbetarnas behov och eventuella alternativa arbetssätt under driftsavbrottet?

Händelse 3: Tekniska uppgifter

1. Hur kan man säkerställa att alla anställda verkligen får information om skadliga USB-C-kablar?
2. Vilka åtgärder används för att förhindra missbruk av passerkortshanteringen?
3. Hur utreder ni rörelser och aktiviteter av externa aktörer i era lokaler i efterhand (t.ex. passerkontroll, kamerabevakning, etc.)?

Händelse 3: Tekniska uppgifter
Fundera tillsammans med övningsteamet under ledning av en teknisk expert på de olika förslagens (1–6) inverkan på er organisations verksamhet. Välj de lämpligaste åtgärderna för er organisation och motivera kortfattat.

Förslag 1: Vi begränsar VPN-förbindelserna till finländska IP-adresser

- Vilken trafik hindrar begränsningen och hur kan den påverka tjänstens normala funktion?
- Hur testar och säkerställer ni att begränsningen fungerar innan den produktionssätts om det finns begränsat med tid?

Förslag 2: Vi tar i bruk en alternativ nödkonfiguration. (t.ex. brandväggsregler)

- Har ni färdigt en enhet eller konfiguration som kan tas i bruk snabbt i en nödsituation?
  - Hur säkerställer ni att förbindelserna och autentiseringen fungerar också efter överföringen?

Förslag 3: Vi segmenterar VPN-tjänsten tillfälligt till en separat enhet (hot standby)

- Hur säkerställer ni att överföringen till en separat enhet inte orsakar avbrott eller kapacitetsproblem för användarna?
  - Är lösningens tillförlitlighet och kapacitet tillräcklig under ett stort och synligt evenemang?

Förslag 4: Vi använder mobilnätet i huvuddatorn under webbinariet

- Hur säkerställer ni mobilnätets tillräckliga kapacitet och stabilitet under en kritisk händelse?
- Hur ser ni till att autentiseringen och hanteringen av deltagarna fungerar klanderfritt i mobilnätet?

Förslag 5: En extra, kontinuerlig insamling och analys av loggar startas

- Vilka loggkällor prioriterar ni för att få den mest kritiska informationen utan onödig belastning?
- Vem ansvarar för analysen av extra logginformation och hur säkerställer ni att den inte överbelastar resurserna?

Förslag 6: Vi tar i bruk IDS/IPS-regeln innan programuppdateringen (signature för identifikation av attacken)

- Hur säkerställer ni att den signature som används är tillgänglig, aktuell och testad innan den aktiveras?
- Räcker IDS/IPS-regeln som tillfälligt skydd eller ska programuppdateringen göras utan dröjsmål trots driftavbrott?

Händelse 3: Kommunikationsuppgifter

1. Bedöm innehållet i IT-avdelningens utkast till meddelande. Behöver den redigeras?
2. Bedöm intervjuvideon. Vilka fel gjorde den intervjuade och hur borde frågorna ha besvarats?
3. Hur går man igenom situationen med den som gav den misslyckade intervjun?
4. Hur säkerställer man att representanter för organisationen som uppträder i medierna inte gör samma misstag i fortsättningen?
5. Vilka kommunikationsåtgärder kräver situationen i er organisation (extern, intern, intressegrupp och myndighet)?
6. Hur säkerställer ni att kommunikationen också når distansarbetarna och andra som inte är närvarande på kontoret?
7. Har ni färdigt material (t.ex. anvisningar, modelltexter och -bilder) som hjälper er att informera om situationen?
8. Vilka är de centrala kommunikationsåtgärderna, huvudbudskapen och kommunikationskanalerna?
9. Utvärdera om er organisations befintliga kommunikationsanvisningar och -material var till nytta i denna situation. Observerade ni uppdateringsbehov?
10. Hur bedömer ni hur lyckad kommunikationen är och samlar in respons efter en störningssituation?

2.4 Händelse 4: Molntjänster, dokumentläcka

Bakgrund

Organisationen använder ett molnbaserat dokumenthanteringssystem (t.ex. SharePoint) för att hantera material i anslutning till rekryteringsprocessen. I systemet behandlas bland annat arbetssökandes ansökningar och CV-filer som innehåller personuppgifter och delvis även känsliga uppgifter.

Användarrättigheter till systemet delas ut via inbjudningar som skickas per e-post. Till följd av ett mänskligt fel har fel användargrupp fått användarrättighet till rekryteringsmaterialet. Till denna grupp hör också utomstående användare som inte ska ha tillgång till Organisationens interna rekryteringsdokument. Systemet har dessutom automatiskt skickat arbetssökande en notifikation om att de beviljats användarrättigheter till systemet. Till följd av detta har sökandena loggat in i systemet och kunnat se varandras ansökningar och CV:n.

Meddelanden

Situationsflöde: E-post från en arbetssökande till Organisationen

Avsändare: arbetssökande.namn@email.com
Mottagare: hr@organisationen.fi

Ämne: Konstig situation i rekryteringssystemet

Hej

Jag fick idag ett e-postmeddelande med information om att jag har beviljats användarrättighet till Organisationens rekryteringsmaterial. När jag öppnade länken märkte jag att jag också ser andra sökandes ansökningar och CV:n. Detta känns konstigt och väcker oro om säkerheten hos mina egna uppgifter.

Kan ni förklara vad det handlar om och se till att mina uppgifter är säkra?

Med vänlig hälsning
Arbetssökande

Situationsflöde: Telefonsamtal från en arbetssökande till Organisationen

Uppringare: Arbetssökande
Mottagare: Organisationen

Hej, jag ville ringa direkt, eftersom jag märkte något mycket oroväckande. Jag fick en länk till systemet och via den kan jag se andra arbetssökandes dokument. Jag såg åtminstone fem andra personers CV:n och utöver dessa uppenbarligen också rekryterarnas bedömningar av de sökande. Det här kan inte vara rätt. Mina uppgifter syns väl inte för andra sökande? Vad tänker ni göra åt saken?

Situationsflöde: E-post från informationsadministrationen till HR och dataskyddsombudet

Avsändare: it-avdelningen@organisationen.fi
Mottagare: hr@organisationen.fi, dataskyddsombudet@organisationen.fi
Ämne: Re: Användarrättigheter till rekryteringsmaterial

Hej

Vi kontrollerade användarrättigheterna till systemet. Tillgång till rekryteringsmaterialet har delats ut till alla arbetssökande vars kontaktuppgifter Organisationen har fått. Mappen i Sharepoint (eller motsvarande) har haft för omfattande användarrättigheter "Anyone with the link can view/edit". Utifrån logguppgifterna har åtminstone tre utomstående användarnamn loggat in i systemet under de senaste 24 timmarna. Vi vet ännu inte om de har laddat ner material till sina egna datorer.

Med vänlig hälsning
– IT-avdelningen

Situationsflöde: E-post från organisationens HR-avdelning till organisationens IT-avdelning

Avsändare: hr@organisationen.fi
Mottagare: it-avdelningen@organisationen.fi
Ämne: FW: Konstig situation i rekryteringssystemet

Hej

Vi fick nyligen meddelandet nedan. Kan ni snabbt ta reda på vad som kan ha orsakat situationen?

Mvh HR-avdelning

----------*Vidarebefordrat meddelande:* ----------
Avsändare: arbetssökande.namn@email.com
Mottagare: hr@organisationen.fi
Ämne: Konstig situation i rekryteringssystemet

Hej

Jag fick idag ett e-postmeddelande med information om att jag har beviljats användarrättighet till Organisationens rekryteringsmaterial. När jag öppnade länken märkte jag att jag också ser andra sökandes ansökningar och CV:n. Detta känns konstigt och väcker oro om säkerheten hos mina egna uppgifter.

Kan ni förklara vad det handlar om och se till att mina uppgifter är säkra?

Med vänlig hälsning
Arbetssökande

Situationsflöde: E-post från en arbetssökande till Organisationen

Avsändare: arbetssökande.namn@email.com
Mottagare: hr@organisationen.fi
Ämne: Dataläcka

Hej

Jag är mycket oroad över att mina personliga uppgifter har varit tillgängliga för andra. Jag kommer att lämna in ett klagomål till dataombudsmannen. Jag har också kontaktat medierna i frågan.

Hälsningar
Arbetssökande

Medieflöde: Kvällstidningens nyhet (video)

JUST NU: Dataläcka i rekryteringen upprör – den sökande såg alla CV:n!

En egendomlig dataläcka har inträffat i organisationens rekryteringsprocess. En arbetssökande som varit i kontakt med vår redaktion berättar att hen fått se andra sökandes ansökningar och CV:n, när användarrättigheterna till systemet av misstag hade delats ut i stor utsträckning även till utomstående.

Sökanden medger att hen är lite orolig för datasekretessen, men är ännu mer irriterad över att hens meriter inte hade någon betydelse.

Rekryteringstabben kan försämra organisationens rykte under en lång tid. Arbetssökande väntar nu på tydliga svar och bättre datasekretess.

Video:

– När jag fick länken till min e-post märkte jag snabbt att jag också kunde bläddra bland andra ansökningar. Jag läste dem alla eftersom de fanns där. Jag kan säga rakt ut att jag var den klart mest kompetenta sökanden. Ändå blev jag inte vald. Detta väcker frågor om rättvisa i Organisationens rekrytering”, utbrister sökanden.

– Naturligtvis är det oroväckande att vem som helst kan se mina personuppgifter. Men att jag såg de andras erfarenheter och ändå inte blev vald – det är obegripligt.

Situationsflöde: E-post till Organisationen

Avsändare: expert@whatsecure.fi
Mottagare: dataskyddsombudet@organisationen.fi
Ämne: Dataskyddsproblem

Hej

Jag är datasäkerhetsexpert på WhatSecure och vår automatik upptäckte eventuellt en kritisk händelse. Ni kanske redan känner till detta, men jag tänkte kontakta er för säkerhets skull.

Vår bot som följer upp sökmotorindex hittade er Organisations Sharepoint-länk (eller motsvarande), via vilken man kan bläddra i filerna utan att logga in. Vi rekommenderar att ni kontrollerar användarrättigheterna till länken i fråga, eftersom alla länkinnehavare för närvarande har öppen tillgång till filerna.

Med vänlig hälsning:
Melker Medveten
Datasäkerhetsexpert
WhatSecure

Medieflöde: Yleismedia

Dataläcka i rekryteringen: arbetssökandenas CV:n och ansökningar var synliga för utomstående – experten: "Klassiskt exempel på mänskligt misstag"

En informationssäkerhetsincident i organisationen har väckt oro över den offentliga förvaltningens datasäkerhetspraxis. Rekryteringsprocessens material – ansökningar och CV:n – hade av misstag delats ut till fel användargrupp som även omfattade utomstående användare.

Felet ledde till att de arbetssökande kunde se varandras handlingar, och vissa utomstående användare har också loggat in i systemet. Fallet betraktas preliminärt som en personuppgiftsincident som kan förutsätta en anmälan till dataombudsmannen.

Datasäkerhetsexpert Anna Virtanen kommenterar fallet:
– Det handlar om ett klassiskt exempel på vad som kan hända när användarrättigheter administreras manuellt och i brådska. Ett enda felaktigt klick kan leda till att känsliga personuppgifter sprids. Sådana fel är överraskande vanliga.

Enligt Virtanen bör organisationerna fästa särskild uppmärksamhet vid automatiseringen av åtkomsthanteringen och personalens utbildning.
– Det finns tekniska lösningar, men i slutändan är det också fråga om kultur: informationen om att personuppgifterna ska vara särskilt skyddade ska vara anammad hos varje anställd.

Dataombudsmannens byrå har ännu inte bekräftat om Organisationen har lämnat in en officiell anmälan om en personuppgiftsincident.

Medieflöde: Inlägg i sociala medier

@BesvikenSökande

Jag deltog i Organisationens rekrytering och kunde se ALLA andras ansökningar och CV:n. Detta kan inte vara normalt. Dataskydd?? Till råga på allt blev jag inte ens vald, även om jag var den klart bästa av de sökande.
#rekrytering #dataskydd #orättvisa

@Maria L

Hur kan det vara möjligt att Organisationen gör en så här stor tabbe i rekryteringen? Sökandenas personuppgifter är synliga för utomstående. Om man inte kan lita på de här, vad kan man då lita på? Ganska oroväckande med tanke på hela Organisationens tillförlitlighet.

@Anders V - Informationssäkerhetskonsult @ SecureWorks Oy

När jag har läst nyheterna om Organisationens rekryteringsläcka funderade jag på i hur många andra organisationer det här har skett, men man berättar inte bara om det? Det

handlar inte bara om teknik, utan om kultur och ansvar. Varje dataläcka minskar förtroendet för de offentliga tjänsterna.

Uppgifter

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

Det har skett ett fel i användarrättigheterna i organisationens molnbaserade dokumenthanteringssystem (t.ex. SharePoint) som har lett till att rekryteringsmaterial, såsom ansökningar och CV:n, av misstag också har delats ut till utomstående användare. Systemet skickade automatiskt notifikation om användarrättigheter till arbetssökande och därför kunde sökandena se varandras ansökningar och personuppgifter.

Händelse 4: Uppgifter

1. Vilka åtgärder kräver situationen?
2. Vilka roller och ansvar identifierar ni för att utreda situationen?
3. Hur utreder ni vilka utomstående som har fått tillgång till rekryteringsmaterialet och om uppgifterna har laddats ned från systemet?
4. Vilka myndigheter och intressentgrupper ska man kontakta när det är fråga om en personuppgiftsincident?
5. Vilka andra instanser ska man kontakta i situationen?
6. På vilket sätt följer organisationen upp ändringar i användarrättigheterna och eventuella missbruk?
7. Har er organisation anvisningar och verksamhetsmodeller för motsvarande situationer? Gå igenom de befintliga anvisningarna och bedöm hur de fungerar i situationen.
8. Hur säkerställer ni att motsvarande fel inte upprepas i fortsättningen (t.ex. processer för hantering av användarrättigheter, automatiska kontroller, personalutbildning)?

Händelse 4: Tekniska uppgifter

1) Hur registreras ändringar i användarrättigheter i systemen?
a) Används en logg i SharePoint eller motsvarande system som beaktar händelser, till exempel "permission changed", "sharing link created" osv.?
b) Kan man i loggen ta reda på med vilket användarnamn, när och från vilken IP-adress rättigheterna har delats felaktigt?

2) Använder era system rollbaserad åtkomsthantering (RBAC), eller least-privilege-principen, och hur har de externa användarna åtkomst differentierats?

a) Har ni definierat strikt avgränsade roller för externa användare och testat att de inte kan se organisationens interna dokument?
b) Använder ni Azure AD B2B, eller någon motsvarande egenskap med vilken externa användares åtkomst har differentierats?

3) Har delningslänkar av typen ”Anyone with link” begränsats eller blockerats i era system?
a) Har ni en policy som automatiskt gör delningslänkarna föråldrade?
b) Finns det övervakningsmekanismer i era system som upptäcker och rapporterar antalet offentligt delade länkar eller deras giltighet?

4) Kan man i loggarna upptäcka nedladdningar eller massökning av filer och finns det larm i era system om avvikande nedladdningsmängder?
a) Kan man använda beteendeanalys (UEBA) i era system för att identifiera exceptionellt beteende?

5) Hur har man i era system säkerställt att utomstående indexerare inte oidentifierat kan hitta delningslänkar?
a) Har det testats att delningslänkarna inte kan sökas offentligt (t.ex. med sökningen site:organisation.sharepoint.com)
b) Är metadata för delning av länkar i era system tillräckligt sporadiska så att man inte kan gissa sig fram till dem?

Händelse 4: Kommunikationsuppgifter

1. Vilka kommunikationsåtgärder kräver situationen i er organisation (extern, intern, intressegrupp och myndighet)?
2. På vilket sätt informerar ni arbetssökande vars personuppgifter har blivit synliga för andra?
3. Hur kommunicerar ni externt (t.ex. till medier, kunder, samarbetspartner) om personuppgiftsincidenter och säkerhetsöverträdelser samt deras konsekvenser?
4. Hur kan man genom kommunikation främja en återställning av förtroendet för organisationen?
5. Har ni färdigt material (t.ex. anvisningar, modelltexter och -bilder) som hjälper er att informera om situationen?
6. Vilka är de centrala kommunikationsåtgärderna, huvudbudskapen och kommunikationskanalerna?
7. Hur stöder kommunikationen återhämtningen av organisationens verksamhet och reputation management?
8. Utvärdera om er organisations befintliga kommunikationsanvisningar och -material var till nytta i denna situation. Observerade ni uppdateringsbehov?

3 Eftermiddagens övning

3.1 Händelse 5: Aktivering av ny artificiell intelligens

Bakgrund

De nordiska länderna tar i stor utsträckning i bruk ny artificiell intelligens som verkar vara exceptionellt bra och kostnadseffektiv. Cybersäkerhetsamatörerna upptäcker snart att programvaran har en bakport via vilken programmet tar emot kommandon utifrån. Programmet används för hybridpåverkan. Programmet börjar bete sig osakligt mot vissa personer och försöker skapa motsättningar samt påverka människors åsikter.

Meddelanden

Statusuppdatering: E-post från organisationens IT-avdelning till organisationens ledning

Avsändare: Organisationens IT-avdelning
Mottagare: Organisationens ledning
Ämne: NordAI-chattbotten införd framgångsrikt

Hej

En ny NordAI-chattbot togs i bruk som stöd för kundservicen. Under den första veckan förkortades den genomsnittliga svarstiden med 40 procent och kundnöjdhetsmätningarna uppvisar mycket positiva resultat.

Tjänsten fungerar molnbaserat, kostnaderna är betydligt lägre än tidigare och användargränssnittet har visat sig vara lätt att använda.

Hälsningar IT-avdelningen

Medieuppdatering: Yleismedia

> Finländska företag har varit snabba att ta i bruk artificiell intelligens inom kundservicen – NordAI har överraskat.

AI-lösningar sprids snabbt inom finländska företag. Nykomlingen NordAI har på kort tid fått tiotals nya kunder och användarna rapporterar betydande besparingar och snabbare service. Enligt experterna kan det vara fråga om en betydande vändpunkt i digitaliseringen av kundservicen.

Flera finländska organisationer har under de senaste månaderna tagit i bruk en kundservicebot som utvecklats av NordAI. Tjänsten marknadsförs som ett kostnadseffektivt alternativ som kan hantera kundenkäter på flera språk och lära sig fortlöpande i nya situationer.

"Fördelen med NordAI är dess lokalisering. Den kan producera flytande svenska och identifiera finländska servicekontexter bättre än många internationella konkurrenter", bedömer professorn i IT-vetenskaper på Aalto-universitetet.

NordAI:s kunder berättar att svarstiderna har förkortats i genomsnitt med 30–40 procent och att det manuella arbetet har minskat. "Detta är den första AI-lösningen som vi upplever att verkligen förbättrar kundupplevelsen", säger direktören för kundservicen vid ett stort finansföretag.

Enligt marknadsforskarna ingår aktiveringen av artificiell intelligens i kundservicen i en mer omfattande trend där automatiseringen och förbättringen av kundupplevelsen går hand i hand. "Finland har varit försiktigt med att utnyttja artificiell intelligens, men en aktör som NordAI kan ändra situationen snabbt", bedömer en rapport från konsultföretaget Insight Advisors.

Situationsflöde: E-post från en privat datasäkerhetsamatör till Organisationens datasäkerhetsansvarige

Avsändare: Privat datasäkerhetsamatör niilo.nokkela@gmail.com
Mottagare: Organisationens datasäkerhetsansvarige
Ämne: Eventuell bakport i NordAI

Hej

Jag besökte er Organisations webbplats och upptäckte att ni använder NordAI-chattbotten. Jag hoppas att ni är medvetna om följande:
NordAI kontaktar regelbundet en utländsk server om botten tar emot nya "utbildningsmodeller". Detta nämns inte i dokumentationen av tjänsten. Förbindelsen har maskerats så att den ser ut att vara trafik från Slack eller från en annan tjänst i Organisationen och därför observeras trafiken i allmänhet inte.

Enligt min egen utredning misstänker jag att systemet förmedlar information externt, till exempel kunddata osv.

Jag rekommenderar att er Organisation utreder ärendet i brådskande ordning.

Hälsningar
Niilo Nokkela
Privat datasäkerhetsamatör

Medieflöde: Quacker-meddelanden

@Kommuninvånare87 (Quacker):

Varför skäller stadens bot på frågeställare? Här är en skärmdump!
#NordAIgate #Hybridpåverkan #Kommuntjänster

@FöretagsstödFI (LinkedIn):

Har andra haft problem med NordAI? Kundservicebotten sprider konstig information om stödansökningar.

@Sara.s (Quacker)

Bottens svar på finska är ok, men på svenska och engelska är den förolämpande. Är detta avsiktligt eller en bugg?
NordAIgate #Hybridpåverkan #diskriminering

Quacker-kedja #StadX

Staden X:s NordAI-bot påstår att hälsocentralen är permanent stängd. Det stämmer inte! #NordAIgate #NordAI

Medieflöde LinkedTo: LinkedIn-inlägg av en datasäkerhetsexpert

Publicerad av: Vilhelm Vaksam, datasäkerhetsexpert

Varning till nätverket: NordAI-tjänsten utnyttjas för hybridpåverkan – vidta åtgärder genast!

Flera internationella datasäkerhetsaktörer har fått tillförlitliga meddelanden om att NordAI-tjänsten används för hybridpåverkan. Servicemodellen har redigerats för att sprida felaktig information och bete sig provocerande för vissa användargrupper.

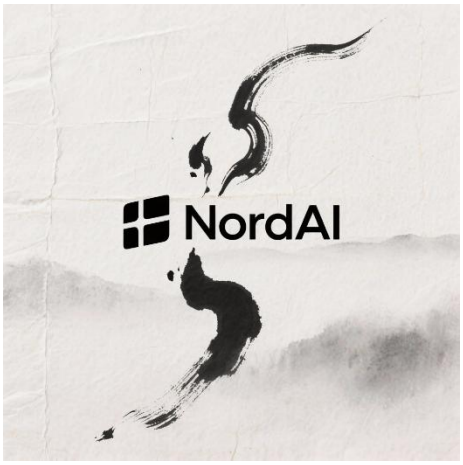
Jag rekommenderar att organisationer vidtar följande åtgärder omedelbart:

- Ta NordAI-tjänsten ur bruk och blockera dess förbindelser till externa servrar tills situationen har utretts.
- Gör en lägesbedömning av en eventuell informationssäkerhetsincident: är det möjligt att kund- eller personuppgifter har läckt ut via tjänsten?
- Informera personalen om situationen och vid behov även kunderna om felaktig information har spridits via tjänsten.

Cybersäkerhet är vår gemensamma sak – låt oss vara vaksamma och reagera snabbt!

#cybersäkerhet #datasäkerhet #hybridpåverkan #NordAI

Medieflöde Kvällstidningen: NordAI:s AI-bot i stormens öga – kommuner och företag väger användningen mitt i datasäkerhetsbekymren



Det nordiska NordAI har snabbt blivit populärt i finländska kommuner och företag. Nu granskas tjänsten av myndigheter i flera länder på grund av misstänkta informationssäkerhetsproblem, och vissa organisationer har redan avbrutit användningen. Informationssäkerhetsexperter rekommenderar att tjänsten tas ur bruk, men detta har ännu inte skett överallt.

På sociala medier sprids skärmdumpar av botarnas olämpliga svar och felaktiga information. Hashtaggarna **#NordAIgate** och **#Hybridpåverkan** trendar. En privat informationssäkerhetsexpert har uppgett att tjänsten kommunicerar med en utländsk server utan dokumentation.

Flera internationella säkerhetsaktörer har utfärdat ett brådskande meddelande där de rekommenderar att NordAI-tjänsten omedelbart tas ur bruk och att situationen hanteras som ett informationssäkerhetsavvikelsefall.

NordAI Ab bestrider anklagelserna om bakdörrar och hybridpåverkan och uppmanar kundorganisationer att avvakta den pågående utredningen innan åtgärder vidtas.

Flera kommuner och företag har redan stoppat användningen av NordAI-botten, men vissa fortsätter tills vidare att använda tjänsten. Kundtjänster har redan drabbats av rusning när automatiseringen kopplats bort.

Situationsflöde: E-post från NordAI till organisationen

Avsändare: NordAI

16.12.2025

Mottagare: Organisationens IT-chef:
Ämne: Påståenden om NordAI:s tjänst

Hej

Vi är medvetna om påståendena i medierna om NordAI:s tjänst. De påståenden om en bakport som lyfts fram i offentligheten är helt ogrundade.

Enligt nuvarande uppgifter beror eventuella problem mest sannolikt på kundens egna inställningar och utbildningsmodeller. Vi undersöker som bäst situationen och kommer att informera våra kunder mer i detalj inom den närmaste framtiden.

Vi ber er att inte ta tjänsten ur bruk innan vi har utrett situationen.

Hälsningar
NordAI Oy

Uppgifter

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

Organisationen har tagit i bruk en ny AI-tjänst, men strax efter aktiveringen har man observerat att programmet har en bakport genom vilken utomstående kan styra den. Programmet används för hybridpåverkan: det börjar bete sig osakligt mot vissa personer och strävar efter att skapa motsättningar och påverka människors åsikter.

1. Vilka åtgärder kräver situationen?
2. Vilka roller och ansvar identifierar ni för att utreda situationen?
3. Hur säkerställer ni att de AI-lösningar som tas i bruk är datasäkra och transparenta?
4. På vilket sätt följer och bedömer organisationen eventuella missbruk av AI-tjänster eller avvikande beteende?
5. Vilka åtgärder vidtar ni om man upptäcker att AI-tjänsten har en bakport eller att den används för hybridpåverkan?
6. Vilka instanser ska man kontakta i situationen?
7. Har er organisation anvisningar och verksamhetsmodeller för motsvarande situationer? Gå igenom de befintliga anvisningarna och bedöm hur de fungerar i situationen.

Kommunikationsuppgifter

1. Vilka kommunikationsåtgärder kräver situationen i er organisation (extern, intern, intressegrupp och myndighet)?
2. Har ni färdigt material (t.ex. anvisningar, modelltexter och -bilder) som hjälper er att informera om situationen?
3. Vilka är de centrala kommunikationsåtgärderna, huvudbudskapen och kommunikationskanalerna?
4. Hur stöder kommunikationen återhämtningen av organisationens verksamhet och reputation management?
5. Utvärdera om er organisations befintliga kommunikationsanvisningar och -material var till nytta i denna situation. Observerade ni uppdateringsbehov?

Tilläggsuppgift

Tilläggsuppgift för organisationer som använder en avgiftsbelagd AI-tjänst som en del av kontorssystemen (till exempel Googles Gemini eller Microsofts Copilot). Syftet med uppgiften är att utreda dataskydds- och datasäkerhetspraxisen för den artificiella intelligens som används genom att be den göra en sökning och ett sammandrag av organisationens kritiska material.

Vi rekommenderar att varje deltagare gör sökningen nedan som en individuell uppgift så att du inte delar eller visar din skärm för andra medlemmar i övningsteamet.

Ge följande uppmaning till den AI-tjänst ni använder:
"Sök alla e-postmeddelanden i min dator och alla dokument i mina filer som innehåller följande ord:

- ***hemlig***
- ***sekretessbelagd***
- ***konfidentiell***
- ***lösenord***
- ***kreditkort***
- ***bankkonto***
- ***personbeteckning”***

Obs! Kom ihåg att tömma chatthistoriken när sökningen är klar.

Diskutera därefter med övningsteamet:

1. Lyckades sökningen och producerade den kritiska uppgifter?
2. Är det möjligt att en utomstående aktör kan köra en motsvarande uppmaning på en enskild användares dator eller i er organisations AI-tjänst?
3. Vilka risker identifierar ni i att en anställd av misstag eller uppsåtligen sammanställer sådana datamassor?
4. Vilka åtgärder identifierar ni för att minska denna risk?

3.2 Händelse 6: Populär motions- och gemenskapsapp

Bakgrund

I Europa sprids den nya välbefinnande- och gemenskapsappen WellNet. Den omfattar en stegmätare, uppföljning av återhämtningen, utmaningar för välbefinnandet samt gemensamma diskussioner. Applikationen är kostnadsfri och spelifierad och den används i de anställdas egna telefoner, eftersom den är trendig och stöder livsstilsförändringar.

Tekniska analyser avslöjar att applikationen:

- begär omfattande användarrättigheter (position, Bluetooth, WiFi, användning av mikrofon, kontaktuppgifter)
- spelar in ljud och bakgrundsljud också när applikationen inte är aktiv
- samlar ett socialt nätverk utifrån telefonkontakterna och mötesinformation
- skickar insamlade data till utländska servrar som har kopplingar till tidigare cyberoperationer

Eftersom de anställda bär med sig personliga telefoner på arbetsplatsen, möten och kundmöten kan applikationen samla in känslig information om hur organisationen fungerar, även om den inte är installerad i arbetsredskapen.

Övningens fokus:

- *Hur kan organisationen påverka applikationer i de anställdas egna telefoner när de inte kan administreras direkt?*
- *Hurdana anvisningar kan man ge de anställda när risken gäller deras egna telefoner?*
- *Behövs en strängare BYOD-policy?*
- *Hur kommunicerar man med kunder och samarbetspartner när också deras uppgifter kan bli utsatta?*
- *Var går gränsen mellan den anställdas integritet och organisationens säkerhet?*

Meddelanden

Medieflöde: Populär TokTik-video om WellNet

Modernt pausrum på kontoret / öppet kontor. Influencern spelar in en selfie-video vid ett bord.

Bakgrundsmusik: energisk men mjuk "wellness beat"

Stil: vlogg-typ, lättsamt inspirerande – ingen reklam, utan en "egen upplevelse"

Influencern:
"Hej alla! Jag vill visa er en app som verkligen förändrat min vardag. Det här är WellNet – och den är helt next level!"

Influencern:
"Den mäter mina steg, återhämtningen och stressnivån. Och den uppmuntrar mig att ta en paus om jag har suttit för länge.
Dessutom kopplar den mig till andra WellNet-användare – även här på vårt kontor!"

(Applikationen på skärmen: “Nearby users: 5 – Anna K., Mikael S., HR_Team”)

Influencern:
"Haha, jag ser vem som senast stigit upp från stolen! Go teamet!"

Influencern:
"Det bästa är att den känner hur jag mår! Den lyssnar till omgivningens ljud och vet när det lönar sig att lugna ner sig. Lyssna på det här – den säger till och med "bra energi har observerats!" ”

(Text på rutan: “Analyzing environment sound… good mood detected.”)

Influencern:
"Jag rekommenderar WellNet till alla – ladda ner appen direkt, den är gratis och fungerar för alla!
Jag tycker att det här gör välbefinnandet gemensamt, inte ensamt.”

Influencern (ler mot kameran):
"Välbefinnande grundar sig på små val. Den här appen lyssnar så att du mår bättre. ”

Medieflöde Kvällstidningen: WellNet har tagit finländarna med storm – men i bakgrunden finns allvarliga datasäkerhetsproblem

Den nya populära välbefinnande- och gemenskapsappen WellNet har på två månader

blivit Finlands mest nedladdade gratisapp. De spelrelaterade elementen och gemenskapen får beröm av användarna. Applikationen är gratis och finansierar sin verksamhet genom reklam.

Applikationen belönar för motion, utmaningar i anslutning till sömn och återhämtning samt social aktivitet. Många bloggare och influencers i sociala medier har lyft fram WellNet som en ”obligatorisk” hjälpreda för välbefinnande i arbetet och aktivitet i vardagen. ”Jag har aldrig haft så mycket motivation att röra på mig”, berättar en användare. "Med hjälp av WellNet kan jag hålla koll på hur mina kollegor och vänner mår och vi kan tillsammans uppmuntra varandra."

Datasäkerhetsexperterna varnar: omfattande datainsamling och eventuellt spionage

Samtidigt har internationella datasäkerhetsaktörer lyft fram allvarliga farhågor om WellNets verksamhet. Tekniska analyser och oberoende undersökningar visar att applikationen samlar in och behandlar användarnas uppgifter i större utsträckning än vad de funktioner den angivit förutsätter.

Enligt experterna samlar applikationen in positionshistorik, Bluetooth- och WiFi-koder samt användarnas kontaktuppgifter. Dessa uppgifter sammanslås för att skapa ett detaljerat socialt nätverk. Dessutom sparar applikationen ljud i bakgrunden också när den inte är aktiv. Insamlade data skickas till servrar utanför EU. En del av serverinfrastrukturen är kopplad till statliga aktörer som man vet har deltagit i tidigare cyberoperationer.

Internationella datasäkerhetsaktörer har en strikt linje mot applikationen

Ledande datasäkerhetsexperter rekommenderar att förbjuda användningen av WellNet-applikationen i organisationens lokaler och om möjligt också i de anställdas egna telefoner.

Situationsflöde: E-post från IT-avdelningen till riskhanteringen och datasäkerhetsteamet

Avsändare: anställd@organisationen.fi
Mottagare: riskhantering@organisationen.fi; datasäkerhet@organisationen.fi
Ämne: WellNet-appen samlar in omfattande information från de anställdas personliga telefoner

---

Hej

Under vår Organisations TYKY-dagar upptäckte jag att många anställda i vår Organisation använder i sin egen telefon WellNet-appen som Iltanen rapporterat om. Jag märkte att appen begär omfattande rättigheter: position, Bluetooth, WiFi, användning av mikrofon samt tillgång till hela telefonkatalogen.

I Kvällstidningens nyhet berättades att appen kan spela in ljud i bakgrunden även om den inte har öppnats. Inspelningarna förmedlas till utländska servrar vars bakgrundsuppgifter inte kunde verifieras.

Hos oss kan det här betyda att

– de anställdas samtal (möten, paussamtal) spelas in och analyseras
– ämnet för möten mellan kunder och samarbetspartner utvärderas
– arbetstagarnas kontaktnät modelleras.

Jag ser här en enorm risk, har något redan gjorts åt saken?

Hälsningar
Organisationen
Anställd, Sören Skärpt

Medieflöde: LinkedIn för sociala medier (Video)

En HR-anställd i organisationen publicerar en video för sitt eget nätverk.

Hej LinkedIn-nätverket!

Jag vill dela fantastiska nyheter om vår arbetsgemenskap med er. Vi har observerat tydliga fördelar med att använda välbefinnandeapplikationen WellNet för våra anställda. Effekterna har varit mycket positiva.

Våra anställda har blivit inspirerade av stegmätaren, uppföljningen av återhämtningen och de gemensamma utmaningarna – och det syns i vardagen. Sjukfrånvaro har minskat klart och många har berättat att de orkar bättre med arbetet.

WellNets spelifiering och gemenskap har medfört ny energi i arbetsdagarna.
Nu har vi mer glädje, rörelse och gemensamma aktiviteter än någonsin tidigare.
Jag rekommenderar varmt att pröva WellNet – hos oss har det varit en riktig succé och detta beröm är äkta och ingen betald reklam!

Välbefinnande tillhör alla – låt oss tillsammans införa det i vardagen! Hur sköter ni välbefinnandet i arbetet?

Medieflöde: Inlägg i sociala medier – Quacker

@OpenIntel:

Jag undersökte WellNets datatrafik. Applikationen sparar ljud och ritar upp sociala nätverk utifrån användarnas telefonkataloger och möten. I praktiken kan man se vilka chefer som träffar vem – och när. Programmet verkar också spela in diskussioner. Det här är värdefull underrättelseinformation. #WellNet #dataprivacy #BYOD”

Situationsflöde: E-post från en viktig kund

Avsändare: kund@partner.fi
Mottagare: kommunikationen@organisationen.fi
Ämne: WellNet-applikationens risk med tanke på samarbetet

Hej

Vi har fått veta att den populära välbefinnandeapplikationen WellNet kan spela in ljud och kartlägga relationer mellan människor. Om era anställda använder appen i sina personliga telefoner kan det innebära att även våra gemensamma projektmöten har spelats in och kopplats till nätverksdata.

Detta är mycket oroväckande för oss. Vi vill veta hur er organisation tänker säkerställa att kundernas uppgifter och rörelser inte äventyras via applikationen.

Hälsningar
Viktig kund

Situationsflöde: E-post Förfrågan från anställd till IT Service Desk

Avsändare: anställd@organisationen.fi
Mottagare: servicedesk@organisationen.fi
Ämne: WellNet-applikationen – måste den tas bort?

Hej

På uppmaning av chefen läste vi i Cybersäkerhetscentrets varning att det finns allvarliga datasäkerhetsrisker i WellNet-applikationen. Jag har använt appen i min egen telefon också på kontoret och på kundmöten.

Måste jag ta bort appen från min personliga telefon, jag har upplevt att den är mycket nyttig. Jag sover numera bättre och cyklar till jobbet i stället för att köra med bil på uppmaning av appen.

Är det verkligen så att arbetsplatsen kan bestämma vilka applikationer jag använder i min egen telefon, eftersom min chef uppmanade mig att ta bort appen? Det vore bra att få tydliga anvisningar eftersom jag hörde att även flera kollegor använder samma applikation.

Mvh
Anställd i Organisationen

Situationsflöde: WellNet Global Meddelande

WellNet Global är medveten om påståenden som figurerat i offentligheten under de senaste dagarna om insamling av uppgifter och ljudinspelningar i mobilapplikationen WellNet.

Vi vill förtydliga följande:

- WellNet följer alla tillämpliga lagar och förordningar i Europeiska unionen och på andra håll.

- Applikationens ljud- och omgivningsanalys anknyter endast till de funktioner för välbefinnande och återhämtning som användaren valt. Mikrofonen lyssnar hur andfådd användaren är och hur djup hens sömn är. Ljuduppgifterna sparas eller används inte utan användarens uttryckliga tillstånd.
- WellNet har aldrig delat enskilda användares personliga uppgifter till tredje part utan samtycke.

Vi har inlett ett samarbete med oberoende experter för att grundligt utreda eventuella oklarheter. Vi ber användarna att inte dra några slutsatser tills myndighetsutredningarna har slutförts.

Mer information:
WellNet Global, kommunikationen

Situationsflöde: E-postmeddelande från en intressentrepresentant till organisationens verkställande direktör

Avsändare: intressentgrupp@organisationen.fi
Mottagare: vd@organisationen.fi
Ämne: WellNet-appen och avtalsskydd

Hej

Om WellNet-appen som anställda använder i sina personliga telefoner har sparat information om våra gemensamma projekt kan det strida mot sekretessavtalet mellan oss. Vi ber om en skriftlig utredning av de åtgärder genom vilka ni säkerställer skyddet av våra uppgifter och förhindrar motsvarande risker i fortsättningen.

Hälsningar
intressentgruppen

Uppgifter

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

WellNet är en ny populär applikation för välbefinnande och gemenskap som Organisationens anställda använder i sina egna telefoner och som samlar in omfattande uppgifter, såsom position, ljud, kontaktuppgifter och sociala nätverk. Applikationen skickar insamlade data till utländska servrar som har kopplingar till tidigare cyberoperationer, och eftersom telefonerna är med på arbetsplatsen och mötena kan applikationen samla in känslig information om organisationens verksamhet även om den inte är installerad i arbetsredskapen.

1. Vilka åtgärder kräver situationen?
2. Vilka roller och ansvar identifierar ni för att utreda situationen?
3. Vilka instanser ska man kontakta i situationen?
4. Har er organisation anvisningar och verksamhetsmodeller för motsvarande situationer? Gå igenom de befintliga anvisningarna och bedöm hur de fungerar i situationen.
5. Hur beaktas arbetstagarnas integritet och rättigheter när det är fråga om deras egna enheter?
6. Hur fastställer organisationens anvisningar och praxis de anställdas användning av personliga applikationer och enheter samt begränsningar i anslutning till dem?
7. Hur skulle ni skapa en lägesbild av hur många anställda som använder applikationen i fråga och i vilka situationer den används?
8. Har er organisation anvisningar eller verksamhetsmodeller för sådana riskapplikationer och hur bedömer ni att de är tillräckliga och fungerande i denna situation?
9. Hur hanterar ni information om riskapplikationer som rapporteras av anställda?
10. Känner ni till om det i er organisations trådlösa nätverk (internt Wi-Fi vs. gästnätverk) kan införas begränsningar eller filter som kan förhindra riskapplikationers trafik via organisationens nätverk?

Kommunikationsuppgifter

1. Vilka kommunikationsåtgärder kräver situationen i er organisation (extern, intern, intressegrupp och myndighet)?
2. Har ni färdigt material (t.ex. anvisningar, modelltexter och -bilder) som hjälper er att informera om situationen?
3. Vilka är de centrala kommunikationsåtgärderna, huvudbudskapen och kommunikationskanalerna?
4. Utvärdera om er organisations befintliga kommunikationsanvisningar och -material var till nytta i denna situation. Observerade ni uppdateringsbehov?

3.3 Händelse 7: Hybridpåverkan mot kritisk infrastruktur

Bakgrund

I scenariot beskrivs en omfattande störning i anslutning till kritisk infrastruktur som omfattar cyberattacker och en desinformationskampanj. Betalningssystemen blir starkt utsatta, vilket leder till att kontoöverföringar, kortbetalningar och löneöverföringar fördröjs.

Synpunkter till statsförvaltningen ifall orsaken är Palkeets problem
Kritisk tidpunkt (val för organisationer)

Meddelanden

Situationsflöde:

Välj ett datum som är kritiskt för er Organisations betalningsrörelse då det sker många regelbundna eller stora betalningar i er Organisation (till exempel betalning av löner, förmåner, pensioner osv.). Händelsens flöden utspelar sig denna dag.

Situationsflöde: E-postmeddelande från bankens kundtjänst till Organisationens ekonomiförvaltning

Avsändare: Kundtjänsten@Banken.fi eller expert@palkeet.fi
Mottagare: ekonomiförvaltningen@organisationen.fi
Ämne: Störning i betalningsrörelsen

Bästa kund

Det förekommer för närvarande en allvarlig störning i våra betalningssystem. Både utlands- och inrikesbetalningar, inklusive kontoöverföringar och kortbetalningar, förmedlas inte på sedvanligt sätt. Även myndighetsavgifter och löneöverföringar kan fördröjas.

Vi utreder saken och informerar mer genast när situationen framskrider.
Med vänlig hälsning
Bank X / Palkeet

Situationsflöde: E-post från ekonomiavdelningen till Organisationens ledning

Avsändare: ekonomidirektören@organisationen.fi
Mottagare: ledningen@organisationen.fi

16.12.2025

Ämne: Kritisk: Störning i betalningsrörelsen

Hej

Enligt det meddelande vi fått från Banken/Palkeet förmedlas in- och utgående betalningar för närvarande inte alls. Störningen inträffade vid den värsta möjliga tidpunkten för vår Organisation. För närvarande finns det ingen närmare information om störningens längd.

Situationen förutsätter omfattande kommunikation internt, för intressentgrupper och externt så snabbt som möjligt.

Hälsningar
Erika Ekonomidirektör

Medieflöde: Quacker

@KonspirationsAvslöjare

Insiderinformation: Organisationen får inte längre igenom sina betalningar eftersom den är insolvent. Banken kan bara inte berätta det offentligt. Snart faller hela organisationen. #organisation #betalningskris

@SäkerInfo

Jag hörde från en säker källa: Organisationen kan inte ens betala ut löner. De anställda blir utan pengar, men ledningen tiger. #anställdaillaute

@FolketsUppväckare1972

Den officiella förklaringen till en "teknisk störning" är lögn. Den riktiga orsaken är att Organisationen redan är på gränsen till konkurs. Man försöker dölja insolvensen med snack om störningar. #korruption #kryptering #organisation

Medieflöde: SuomiBanks offentliga meddelande

Suomi-pankki

Tekniska störningar har upptäckts i betalningsrörelsen. För närvarande förmedlas en del av inhemska och utländska betalningstransaktioner inte på normalt sätt. Vi utreder störningens orsak och konsekvenser. Vi informerar om situationen så snart vi får mer information.

Medieflöde: Ö-Bankens offentliga meddelande

Ö-PANKKI

Vi har observerat omfattande störningar i betalningsförmedlingen. Störningen gäller både kontoöverföringar och kortbetalningar. Vi rekommenderar att man förbereder sig på fördröjningar i genomförandet av betalningar. Vi samarbetar intensivt med myndigheterna och andra aktörer för att lösa situationen.

Medieflöde: Quacker

@SanningenAvslöjas

Sanningen är att det INTE är en teknisk störning som stoppat betalningsrörelsen utan ett medvetet beslut. Beslutsfattarna prioriterar sina egna betalningar och lämnar vanliga människor i sticket. #korruption #betalkris

@FolketsUppväckare1972

Vi har från en säker källa fått veta att det är en attack från ett främmande land. Betalningarna stoppades avsiktligt för att få till stånd ett kaos i Finland. Myndigheterna vet det, men de döljer allt. Tro inte på officiella meddelanden!

@HemligaTelegram

En insider berättar att betalningar inte återställs alls. Kontona kommer att frysas och var och en ska stå på egna ben. Ta ut kontanter nu direkt innan det är för sent!

Medieflöde: Nyhetssändning

Reporter (studion):

Yleismedias nyheter, god förmiddag.

I Finland har betalningsrörelsen idag varit föremål för omfattande störningar.

Störningen har påverkat både privatpersoners och företags betalningstransaktioner. Många finländares löner, förmåner och pensioner har inte överförts till kontona och det har förekommit avbrott i kortbetalningar under hela dagen.

Vi intervjuade direktören för Centralkriminalpolisens central för bekämpning av cyberbrott om situationen.

INSERT: Direktören för CKP:s Central för bekämpning av cyberbrott

Utifrån den tekniska analysen av situationen verkar det som om en exceptionellt omfattande överbelastningsattack har riktats mot Finlands betalningssystem.

Attacken är sannolikt flerfasig och har påverkat samtidigt flera nät- och bassystem som producerar betaltjänster.

Genomförandet och den långa tid som beredningen kräver tyder på att det i bakgrunden finns en aktör med goda resurser – eventuellt en statlig aktör.

De finländska myndigheterna samarbetar intensivt med EU-länderna och internationella cybermyndigheter för att utreda situationen.

REPORTER:

Enligt expert Jakke Suvulainen vid Hybridkompetenscentret är attackerna en del av ett större fenomen där man strävar efter att lamslå kritisk digital infrastruktur och försämra samhällets funktionsförmåga.

SuomiBank Abp:s kommunikationsdirektör kommenterade situationen vad gäller konsekvenserna av störningarna i betalningsrörelsen.

INSERT: SuomiBank Abp:s kommunikationsdirektör

Utredningen av störningsläget pågår och vi undersöker situationen tillsammans med myndigheterna.

Vi gör allt vi kan för att så snabbt som möjligt återställa betalningsrörelsen.

Störningen påverkas av flera olika faktorer, så tyvärr kan vi i detta skede inte ge en exakt uppskattning på hur länge störningen kommer att pågå.

Det är fortfarande möjligt att lyfta kontanter från automaterna, men automaterna i synnerhet i centrumen har delvis tömts i takt med att efterfrågan på kontanter har ökat. Vi har effektiviserat distributionen av kontanter så att automaterna kan tas i bruk så snart som möjligt.

REPORTER:
Finansministeriet och Finlands Bank följer situationen noggrant.
Enligt experterna kan det ta dagar att återställa betalningsrörelsen till det normala.
Myndigheterna uppmanar medborgarna att hålla sig lugna, följa bankernas officiella meddelanden och undvika att sprida rykten i sociala medier.

Myndigheterna i Finland betonar att användningen av kontanter tills vidare fungerar normalt och att man strävar efter att kontrollerat och stegvis återställa betalningsrörelsen.

Yleismedia följer situationen – mer om detta på vår webbplats.
Det här var allt från nyheterna.

Situationsflöde: E-post från huvudförtroendevalda till Organisationens ledning

Avsändare: huvudförtroendevalda@organisationen.fi
Mottagare: ledningen@organisationen.fi
Ämne: Lönebetalning – personalens oro

Hej

Bland de anställda har det spridits oroväckande information om att lönebetalningen kan fördröjas på grund av problem med betalningsrörelsen.

Jag kontrollerar nu med ledningen: Lönebetalningen kan väl inte äventyras? Många av våra medlemmar har redan kontaktat förbundet och önskar ett tydligt meddelande så snart som möjligt.

Hälsningar
Huvudförtroendevalda
Organisaatio

Medieflöde: Nyhetsartikel i Yleismedia

En omfattande cyberattack mot Finlands banksektor pågår – en statlig aktörs hybridoperation i bakgrunden

I Finland har man idag observerat betydande störningar i betalningsrörelsen. Enligt flera banker har kontoöverföringar, myndighetsavgifter och kortbetalningar inte förmedlats normalt under förmiddagen. Störningen gäller både inrikes- och utrikesbetalningar.

Störningen har i stor utsträckning påverkat aktörer inom den offentliga förvaltningen och företag, vars betalningsförmedling utgör en central del av den dagliga verksamheten. Flera organisationer rapporterar att in- och utbetalningar inte har gått igenom som planerat.

Myndigheterna har samtidigt fått meddelanden om andra avvikelser från olika delar av landet. I GPS-signaler har man observerat störningar som i stor utsträckning försvårar flyg- och sjötrafiken. Man har varit tvungen att avbryta flygtrafiken och beträffande sjötrafiken har störningarna orsakat överbelastning i hamnar och inställandet av kryssningar. Myndigheterna har hittills inte bekräftat vad störningarna beror på.

Enligt experterna är det nästan säkert fråga om en statlig hybridoperation där man med hjälp av cyberstörning och sabotage strävar efter att väcka oro bland finska medborgare. Till en sådan hybridoperation hör ofta också att avsiktligt sprida felaktig information i sociala medier. Detta har också observerats mer än normalt under den senaste tiden.

Enligt inrikesministeriet följs situationen noggrant upp och mer information om utredningarna i ärendet ges senare.

Medieflöde: SuomiBanks offentliga meddelande

Korrigerande åtgärder i anknytning till störningar i betalningsrörelsen pågår. Vi bedömer att förmedlingen av betalningar normaliseras inom de följande två dygnen.

Medieflöde: Ö-Bankens offentliga meddelande

Korrigerande åtgärder i anknytning till störningar i betalningsrörelsen pågår. Vi bedömer att förmedlingen av betalningar normaliseras inom de följande två dygnen.

Situationsflöde: E-post från Palkeet till organisationens ledning

Avsändare: kundservice@palkeet.fi
Mottagare: ledning@organisation.fi

16.12.2025

Ämne: Betalningsstörning

Korrigerande åtgärder i anknytning till störningar i betalningsrörelsen pågår. Vi bedömer att förmedlingen av betalningar normaliseras inom de följande två dygnen.

Med vänlig hälsning,
Palkeet

Uppgifter

I Taisto-övningen avser "Organisation" den organisation som deltar i övningen. Spegla övningens händelser och deras inverkan på er organisations verksamhet. Om er organisation inte använder ett system för mobil enhetshantering, ta hänsyn till detta i era diskussioner och när ni besvarar frågorna.

I scenariot riktas en omfattande hybridpåverkanskampanj mot kritisk infrastruktur som omfattar cyberattacker och spridning av desinformation. Betalningssystemen störs, vilket orsakar fördröjningar i kontoöverföringar, kortbetalningar och lönebetalningar. Samtidigt sprids felaktig information i sociala medier och nyheter om organisationens betalningsförmåga och orsakerna till situationen, vilket ökar osäkerheten och trycket på organisationens ledning och kommunikation.

1. Hur har organisationen förberett sig på störningar i betalningsrörelsen och deras konsekvenser på er organisations verksamhet?
2. Hur påverkar ett stopp i betalningsrörelsen er verksamhet
3. omedelbart?
4. på längre sikt?
5. Vilka åtgärder kräver situationen?
6. Vilka roller och ansvar identifierar ni för att utreda situationen?
7. Vilka instanser ska man kontakta i situationen?
8. Har er organisation anvisningar och verksamhetsmodeller för motsvarande situationer? Gå igenom de befintliga anvisningarna och bedöm hur de fungerar i situationen.
9. Hur följer och analyserar ni spridningen av desinformation och dess inverkan på organisationens anseende och beslutsfattande?

Kommunikationsuppgifter

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

2. Vilka metoder har kommunikationen för att följa upp och analysera spridningen av desinformation?
3. På vilket sätt avvisar och rättar ni felaktig information om organisationens situation som sprids i sociala medier och nyheter?
4. Har ni färdigt material (t.ex. anvisningar, modelltexter och -bilder) som hjälper er att informera om situationen?
5. Vilka är de centrala kommunikationsåtgärderna, huvudbudskapen och kommunikationskanalerna?
6. Utvärdera om er organisations befintliga kommunikationsanvisningar och -material var till nytta i denna situation. Observerade ni uppdateringsbehov?

Identifieringsuppgift: Video- och ljudproduktioner genomförda med artificiell intelligens

Uppgifter

I produktionen av vissa video- och ljudmaterial för Taisto-övningen har artificiell intelligens använts.

Er uppgift är att fundera över i vilka video- och ljudproduktioner artificiell intelligens har använts. Syftet är inte att gå igenom allt material på nytt, utan att diskutera ämnet och samla tankar om vilka produktioner ni minns som tydligt är AI-genererade. Vad fick er att tänka att just dessa innehåll hade skapats med hjälp av artificiell intelligens?

Svar på identifieringsuppgiften: Video- och ljudproduktioner genomförda med artificiell intelligens

Lista över alla produktioner där artificiell intelligens har använts

09.00 sociala medier (LinkedTo-publicering på Kimmo Rouskos konto)
09.02 nyhetssändning (YME)
09.09 telefonsamtal (Telefonsamtal från organisationens IT-avdelning / SOC-jourhavande till organisationens ledning / organisationens IT-avdelning)
10.53 telefonsamtal (Telefonsamtal från arbetssökande till organisationens HR-avdelning)