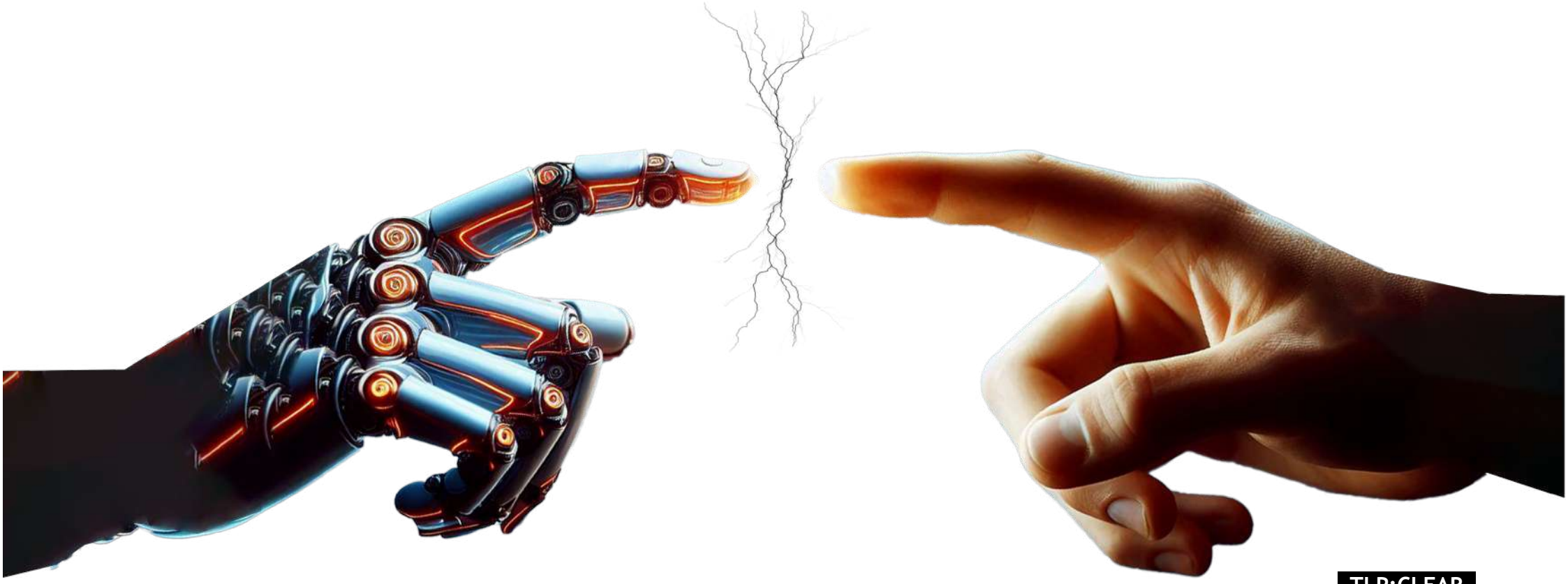
DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

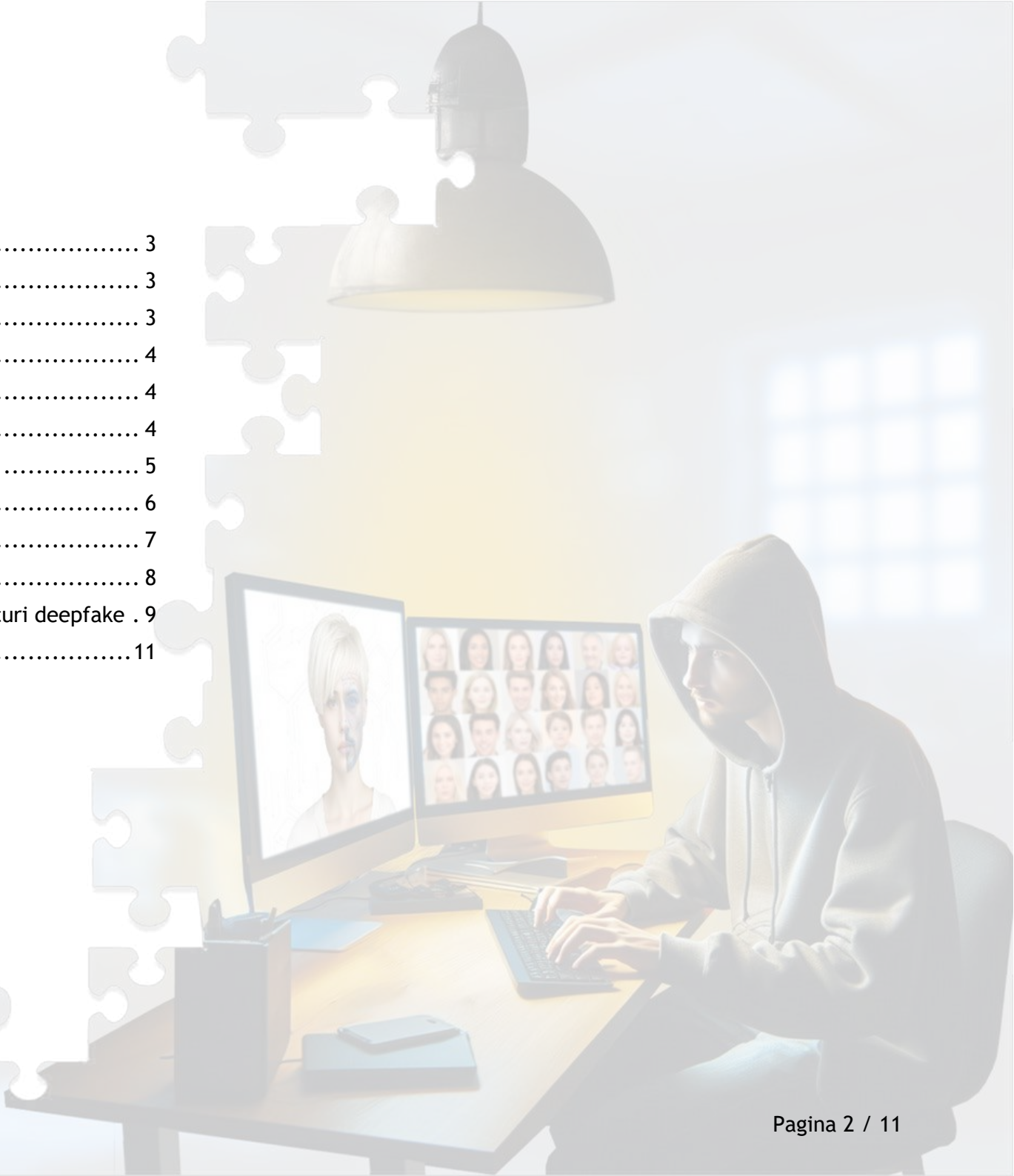
DEEPFAKE

GHID PENTRU ORGANIZAȚII



TLP:CLEAR

Cuprins



Sumar executiv

Tehnologia deepfake aduce riscuri semnificative pentru securitatea și reputația organizațiilor, permițând manipularea conținutului media într-un mod dificil de detectat. Ghidul oferă recomandări pentru prevenirea și gestionarea acestor riscuri, subliniind importanța educației și conștientizării angajaților, utilizării tehnologiilor de detectare a falsurilor și implementării politicilor de securitate. Înțelegerea tehnologiei deepfake și a implicațiilor sale este importantă pentru a ne proteja de potențialele sale efecte negative.

Definiția și explicația tehnologiei Deepfake

Deepfake-urile sunt reprezentări media manipulate digital, în care conținutul original, fie audio, video sau vizual, este alterat pentru a imita sau recrea acțiuni, voci sau fețe ale unor persoane reale, prin tehnici avansate de învățare automată cunoscute sub numele de "deep learning".

Utilizarea deepfake-urilor a evoluat rapid de la divertisment la crearea de videoclipuri în care politicieni, celebrități sau lideri de companii sunt prezentați făcând sau spunând lucruri controversate, până la înregistrări audio ce imită vocea unei persoane pentru a transmite instrucțiuni false sau a comite fraude și imagini manipulate care generează scene compromițătoare sau înșelătoare. Astfel, deepfake-urile reprezintă un risc pentru securitatea cibernetică, având capacitatea de a cauza daune, cum ar fi răspândirea dezinformării, manipularea informațiilor sau afectarea reputației.

Atacurile deepfake sunt acțiuni care, prin utilizarea tehnologiilor de inteligență artificială (IA), creează conținut digital falsificat imagini, videoclipuri sau fișiere audio –care imită conținut sau persoane reale în scopuri malițioase. Atacurile deepfake pot afecta reputația, relațiile comerciale și securitatea financiară a companiilor, având consecințe grave asupra stabilității lor pe termen lung.

Este important să fim critici față de conținutul media pe care îl consumăm și să verificăm întotdeauna autenticitatea informațiilor înainte de a le distribui mai departe.

Scurt istoric și evoluție

Tehnologia deepfake a cunoscut o evoluție rapidă, de la primele videoclipuri create în 2017 până la instrumentele extrem de avansate din prezent, care permit manipularea realistă a conținutului vizual și auditiv. Progresele în domeniul inteligenței artificiale și al algoritmilor de generare a imaginilor/videoclipurilor, alături de puterea de procesare sporită, costurile reduse și accesibilitatea crescută, au transformat această tehnologie într-o amenințare pentru securitatea cibernetică și încrederea în informații.

Pe măsură ce tehnologia avansează, devine tot mai dificil să distingem realul de fals, ceea ce necesită o abordare proactivă din partea organizațiilor și indivizilor pentru a se proteja de potențiale riscuri și abuzuri.

Figură 1 Exemplu de deepfake CEOs[1]

[1] The Express Tribune News

Cadrul legal și de reglementare

România

Dreptul civil: Deepfake-urile pot încălca drepturi precum dreptul la propria imagine, dreptul la viață privată sau dreptul la demnitate. Persoanele ale căror drepturi au fost încălcate pot intenta acțiuni în justiție pentru a solicita despăgubiri sau pentru a cere eliminarea conținutului deepfake.

Dreptul penal: Deși nu există în prezent o legislație specifică care să reglementeze utilizarea deepfake-urilor, anumite articole din Codul Penal pot fi invocate în cazurile în care această tehnologie este folosită în mod ilegal. Principala infracțiune care poate fi invocată în cazul utilizării deepfake-urilor este falsul informatic, însă aceste tehnologii pot fi utilizate și pentru săvârșirea altor infracțiuni, precum înșelăciunea, hărțuirea, șantajul sau pornografia infantilă, contribuind astfel la conturarea elementelor constitutive ale acestor fapte penale. În situații de dezinformare pe scară largă, în care deepfake-urile sunt utilizate pentru a submina siguranța națională, se pot aplica prevederile din Codul Penal referitoare la infracțiuni contra siguranței naționale, cum ar fi răspândirea de informații false.

Legea audiovizualului: Conținutul audiovizual, inclusiv cel realizat prin tehnologia deepfake, poate fi sancționat prin Legea audiovizualului nr. 504/2002, care impune anumite obligații furnizorilor de servicii media audiovizuale, inclusiv în ceea ce privește protecția minorilor și combaterea discursului instigator la ură.

Uniunea Europeană

Legislația europeană a început să abordeze provocările pe care le ridică deepfake-urile și manipularea de conținut digital, deși încă nu există un cadru legal specific și complet pentru această tehnologie. Astfel, diverse inițiative legislative sau norme juridice existente oferă un cadru de reglementare care poate fi aplicat în anumite contexte.

Regulamentul privind inteligența artificială (AI Act) prevede norme pentru utilizarea sistemelor de inteligență artificială. În cadrul acestuia, deepfake-urile sunt clasificate drept sisteme cu risc limitat, iar actul prevede obligații de transparență care obligă ca orice conținut generat de AI, inclusiv deepfake-uri, să fie etichetat sau marcat corespunzător pentru a informa utilizatorii despre natura sa sintetică.

Regulamentul General privind Protecția Datelor (GDPR) reglementează prelucrarea datelor cu caracter personal, inclusiv imaginile, videoclipurile și înregistrările audio utilizate în crearea deepfake-urilor. Deși regulamentul nu face referire directă la deepfake-uri, este relevant pentru protecția datelor personale implicate. Crearea și distribuirea de deepfake-uri fără consimțământul persoanei încalcă principiile GDPR, ceea ce poate atrage amenzi substanțiale.

Legea Serviciilor Digitale (DSA) introduce măsuri de creștere a transparenței și responsabilității platformelor online, având o relevanță directă pentru gestionarea deepfake-urilor. Această lege impune platformelor online mari (de socializare, motoare de căutare) să evalueze și să atenueze riscurile sistemice, inclusiv dezinformarea. De asemenea, legea prevede obligații privind moderarea conținutului manipulat și lupta împotriva dezinformării, ceea ce obligă platformele să implementeze măsuri mai stricte pentru a combate aceste probleme.

Directiva privind drepturile de autor în piața unică digitală (2019/790) protejează drepturile de proprietate intelectuală în mediul digital, fiind relevantă în cazul în care deepfake-urile manipulează conținut protejat fără autorizare. Directiva se aplică în mod special deepfake-urilor care utilizează imagini, videoclipuri sau alte medii protejate fără acordul titularului drepturilor de autor.

Directiva privind serviciile media audiovizuale (AVMSD) stabilește un cadru pentru reglementarea serviciilor media audiovizuale, inclusiv a platformelor de partajare video online, care pot fi folosite pentru a distribui deepfake-uri. Statele membre sunt încurajate să adopte măsuri pentru a proteja utilizatorii împotriva conținutului dăunător, inclusiv materialele înșelătoare sau manipulative de tipul deepfake, care pot afecta securitatea publică sau interesele generale ale utilizatorilor.

Codul de bune practici privind dezinformarea este un cod de conduită voluntar, semnat de platformele majore de socializare, care include și prevederi privind combaterea dezinformării, inclusiv prin deepfake-uri.

Deși legislația începe să abordeze provocările aduse de deepfake-uri, aceasta nu ține pasul cu evoluția rapidă a tehnologiei deepfake, iar persoanele și organizațiile sunt supuse la o serie de riscuri.

Riscuri pentru organizații generate de tehnologia deepfake

Tehnologia deepfake reprezintă o provocare pentru organizații, aducând cu sine riscuri semnificative care necesită o atenție sporită, dintre care evidențiem:

Figură 2 Riscuri generate de tehnologia deepfake

1. **Compromiterea identității.** Deepfake-urile pot fi utilizate pentru a crea imagini, videoclipuri sau înregistrări audio[2] false care imită identitatea angajaților sau a liderilor organizației. Acestea pot fi folosite pentru a accesa neautorizat sisteme critice sau pentru a iniția tranzacții frauduloase[3] punând în pericol integritatea datelor și proceselor interne.
2. **Subminarea comunicării și a încrederii.** Atacatorii pot folosi deepfake-uri pentru a falsifica comunicări interne sau externe, ceea ce poate duce la răspândirea dezinformării în cadrul sau în exteriorul organizației. Aceasta nu doar că poate compromite încrederea între angajați, dar poate și afecta relațiile cu partenerii și clienții, având un impact negativ asupra reputației și stabilității operaționale. În plus, repetarea incidentelor deepfake poate genera o reacție de desensibilizare, reducând capacitatea organizației de a răspunde eficient la amenințări reale[4].
3. **Facilitarea atacurilor de tip spear-phishing.** Deepfake-urile pot face parte din atacuri complexe de inginerie socială, cum ar fi spear-phishing[5], unde atacatorii creează mesaje personalizate și credibile pentru a păcăli angajații să dezvăluie informații sensibile sau să execute acțiuni periculoase. Acestea cresc exponențial riscul de acces neautorizat și de compromitere a rețelelor interne.
4. **Manipularea informațiilor strategice.** Într-o organizație, deciziile strategice depind adesea de informații precise și verificate. Deepfake-urile pot fi folosite pentru a falsifica sau altera mesaje vocale, prezentări sau comunicări, influențând astfel procesul decizional[6]. Acest lucru poate duce la luarea unor decizii greșite, care afectează negativ performanța și direcția strategică a organizației.
5. **Compromiterea sistemelor de securitate.** Pe măsură ce deepfake-urile devin din ce în ce mai sofisticate, încrederea în sistemele de autentificare bazate pe biometrie, cum ar fi recunoașterea facială sau vocală, poate fi compromisă. Atacatorii pot exploata aceste vulnerabilități pentru a obține acces neautorizat la zone securizate, sisteme informatice sau resurse critice ale organizației, punând în pericol securitatea organizației.

[2] Unusual CEO Fraud via Deepfake Audio Steals US$243,000 From UK Company | Trend Micro (US)
[3] Deepfakes: What They Are & How Your Business Is at Risk (bofa.com)
[4] NSA, FBI, and CISA Release Cybersecurity Information Sheet on Deepfake Threats | CISA
[5] Deepfakes: Real threat (kpmg.com)
[6] Deepfake Threats: Survey Reveals Business Impacts

6. **Falsificarea identității în procesele de recrutare și acces.** Tehnologia deepfake poate fi utilizată pentru a crea conținut video sau audio fals, prezentând identități false în diverse etape ale proceselor de recrutare[7], verificare sau autorizare de acces. Acest lucru este deosebit de periculos în contextul interacțiunilor la distanță[8], unde verificarea față în față este limitată, și în relațiile cu terțe părți, precum furnizorii de suport IT extern[9].
7. **Sabotajul sistemelor automate și modelelor IA.** Deepfake-urile pot fi utilizate pentru a manipula sisteme automate de luare a deciziilor, inclusiv modele IA care se bazează pe date video sau audio pentru antrenament sau operațiuni. Prin introducerea de conținut fabricat în aceste sisteme, atacatorii pot modifica rezultatele, pot deteriora seturile de date sau pot induce în eroare algoritmii IA[10].
8. **Manipularea înregistrărilor sistemelor de supraveghere.** Tehnologia deepfake poate fi utilizată pentru a manipula sau fabrica imagini de securitate[11], ducând la narațiuni false sau la mascarea activităților criminale. Atacatorii pot manipula fluxurile video de la camerele de supraveghere pentru a-și ascunde prezența sau acțiunile, sau chiar pot crea imagini false pentru a implica în mod fals o persoană sau o companie.
9. **Subminarea procedurilor legale și a integrității probelor.** Deepfake-urile au potențialul de a crea sau de a modifica dovezi, cum ar fi înregistrări video sau audio, care ar putea fi utilizate în dispute sau investigații legale. Această manipulare subminează integritatea probelor prezentate în instanță, conducând potențial la hotărâri judecătorești sau înțelegeri greșite.
10. **Manipularea conținutului de formare, instruire și educare.** Deepfake-urile pot fi folosite pentru a crea videoclipuri frauduloase de instruire corporativă sau materiale educaționale care par a fi din surse credibile, dar care conțin informații înșelătoare. Acest lucru poate duce la pregătirea inadecvată a angajaților, crescând riscul de erori critice și incidente de securitate în cadrul organizației.

Impactul atacurilor deepfake asupra organizațiilor

Pierderea încrederii și a reputației: utilizarea deepfake-urilor pentru a manipula informații sau comunicații poate duce la pierderea încrederii din partea angajaților, clienților și partenerilor. Odată compromisă, reputația organizației poate necesita timp îndelungat pentru a fi restabilită, afectând relațiile comerciale și veniturile.

Creșterea costurilor de securitate: implementarea măsurilor suplimentare de securitate pentru a detecta și contracara amenințările generate de deepfake implică costuri ridicate. Organizațiile vor trebui să investească în tehnologii avansate de detectare și în instruirea angajaților.

Expunerea la sancțiuni și consecințe legale: manipulările realizate prin deepfake-uri pot expune organizația la riscuri legale, mai ales dacă sunt implicate informații confidențiale sau de proprietate intelectuală. În cazul unor litigii, organizația ar putea fi nevoită să demonstreze autenticitatea informațiilor și a documentelor, ceea ce poate complica și prelungi procesele legale.

Scăderea moralului angajaților: atacurile deepfake care vizează comunicările interne sau imaginea publică a organizației pot avea un efect negativ asupra moralului angajaților. Frica de a fi manipulați sau implicați în incidente de securitate poate reduce productivitatea și crește rata de fluctuație a personalului.

[7] North Korean Hackers Targeted KnowBe4 with Fake IT Worker - Infosecurity Magazine (infosecurity-magazine.com)
[8] Internet Crime Complaint Center (IC3) | Deepfakes and Stolen PII Utilized to Apply for Remote Work Positions
[9] 202404031000_Help Desk Social Engineering Sector Alert_TLPCLEAR (hhs.gov)
[10] Data Poisoning Attacks: A New Attack Vector within AI | Cobalt
[11] Implications of Deepfake Technologies on National Security - Canada.ca

Exemple de incidente deepfake

Pentru a ilustra mai bine impactul concret al deepfake-urilor asupra organizațiilor, vom prezenta câteva exemple notabile de incidente care au avut loc în diferite sectoare:

- Un angajat al unei companii multinaționale a fost indus în eroare și a transferat 25 de milioane de dolari unor escroci care au folosit tehnologia deepfake pentru a se prezenta drept directorul financiar al companiei într-o videoconferință. Escrocii au utilizat deepfake-uri pentru a crea reprezentări video false ale colegilor angajatului, făcându-l să creadă că participă la o întâlnire legitimă[12].
- Într-un incident din 2019, CEO-ul unei companii de energie din Marea Britanie a fost victima unei fraude sofisticate, în care un escroc a utilizat un deepfake audio pentru a imita vocea șefului său german. Atacatorul a reușit să-l convingă pe CEO să transfere suma de 243.000 de dolari. Frauda a continuat cu încă două apeluri în care s-au solicitat plăți suplimentare, însă CEO-ul a devenit suspicios și a reușit să evite pierderi financiare și mai mari[13].
- Un val de reclame false folosește video deepfake cu persoane publice sau companii mari din România pentru a promova investiții care promit câștiguri rapide. Aceste reclame apar pe rețelele sociale și atrag victimele să instaleze programe de control de la distanță, permițând atacatorilor să acceseze aplicațiile bancare ale acestora. Impersonarea companiilor sau a persoanelor publice contribuie la pierderea încrederii publicului și la deteriorarea reputației entităților vizate[14].

[12] https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html
[13] https://www.forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scam-a-ceo-out-of-243000/
[14] https://www.digi24.ro/stiri/actualitate/val-de-fraude-cu-video-deepfake-companii-mari-sau-persoane-cunoscute

Comunicare internă și externă

Comunicarea eficientă și transparentă în timpul unui incident deepfake este esențială pentru a gestiona situația, a preveni escaladarea acesteia, a reduce dezinformarea, a proteja reputația organizației și a menține încrederea părților interesate.

Personalul trebuie informat rapid și clar despre situație, detaliile incidentului, posibilele implicații și instrucțiunile de gestionare a întrebărilor, pentru a asigura un răspuns unitar, coerent și a preveni speculațiile.

Organizația trebuie să emită un comunicat oficial în care să confirme existența incidentului și faptul că se lucrează activ la gestionarea situației, pentru a evita neîncrederea și confuzia create de lipsa unei reacții rapide.

Asigurarea publicului privind analiza tehnică în desfășurare și informarea acestuia și a partenerilor referitor la evoluția situației, fie prin comunicate de presă, postări pe rețelele de socializare sau conferințe de presă. Comunicarea deschisă, proactivă și responsabilă este esențială pentru a minimaliza daunele și pentru a menține încrederea publicului.

Colaborarea între factorii de decizie, experții în comunicare și securitate cibernetică, precum și autorități este esențială în vederea rezolvării problemei, aspect ce arată că situația este tratată cu seriozitate și oferă mai multă credibilitate eforturilor de soluționare.

Este foarte importantă realizarea unei evaluări post-incident a modului în care a fost gestionată comunicarea care să ajute la implementarea unei soluții mai eficiente pentru viitor.

Pentru a proteja reputația organizației și brandul acesteia, dar și pentru a gestiona eficient așteptările publicului și părților interesate în timpul unui incident deepfake, este important să se transmită mesaje clare, coerente și bine structurate.

Mesajele cheie pentru comunicarea de criză în cazul unor incidente de tip deepfake trebuie să reflecte următoarele:

1. **Recunoașterea imediată a situației** - este importantă recunoașterea rapidă a problemei, fapt ce demonstrează informare și implicare, aspect ce va reduce incertitudinile și va împiedica speculațiile să escaladeze.
2. **Asigurarea transparenței situaționale** – asigurarea transparenței ajută la menținerea încrederii părților interesate și la prevenirea apariției de zvonuri și asigură deschiderea și buna intenție a organizației.
3. **Conștientizarea impactului incidentului** – este esențială delimitarea incidentului de valorile și identitatea brandului. Acest mesaj ajută la protejarea reputației pe termen lung.
4. **Informarea publicului privind informațiile verificate din surse oficiale** - redirecționarea publicului către sursele oficiale ajută la combaterea dezinformării și la controlul narativului.

Aceste mesaje, transmise corect și în mod regulat, vor ajuta la minimizarea impactului unui incident deepfake asupra reputației brandului și la menținerea încrederii părților interesate.

Recomandări pentru diminuarea riscurilor generate de atacuri deepfake

Amenințările generate de tehnologiile deepfake pot avea un impact semnificativ asupra organizațiilor, afectând reputația, securitatea și operațiunile. Pentru a gestiona și atenua aceste riscuri, managerii trebuie să adopte o abordare proactivă și integrată. Iată câteva recomandări:

1. Conștientizarea și educarea personalului

- **Training și conștientizare**: Organizarea de sesiuni de instruire pentru angajați privind identificarea și gestionarea conținutului deepfake, pentru ca toți membrii echipei să fie conștienți de riscurile asociate și de modalitățile de răspuns.
- **Actualizări periodice**: Menținerea personalului informat cu privire la cele mai recente tehnici și tendințe în domeniul deepfake prin newsletter-e interne, workshop-uri și materiale educaționale.

2. Implementarea tehnologiilor de detectare și autenticitate

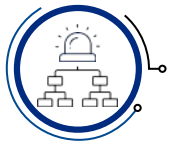
- **Instrumente de detectare**: Adoptarea de soluții software specializate în detectarea deepfake-urilor, care analizează și verifică autenticitatea conținutului media
- **Validarea autenticității**: Utilizarea de tehnologii precum marcaje (watermarks) sau standardele de autenticitate a conținutului Content Authenticity Initiative[15] (CAI) pentru a asigura proveniența și integritatea conținutului media distribuit de organizație.

3. Proveniența conținutului

- **Managementul lanțului de custodie digital**: Implementarea de măsuri eficiente pentru a asigura trasabilitatea și autenticitatea conținutului media folosit în comunicările organizației și stabilirea de protocoale pentru documentarea sursei și istoricului conținutului.
- **Audit și verificare**: Realizarea de audituri periodice pentru a verifica autenticitatea conținutului și pentru a identifica eventualele breșe de securitate.

4. Protejarea datelor sensibile și a personalului cheie

- **Modele Person of Interest (PoI):** Dezvoltarea de modele specifice pentru detectarea deepfake-urilor care vizează persoane cheie din organizație, cum ar fi directori sau lideri de proiect.
- **Colectarea și gestionarea datelor**: Asigurarea că organizația colectează și stochează înregistrări video și audio autentice ale persoanelor de interes pentru a antrena modelele de detecție.



5. Planificare și reacție la incidente

- **Plan de răspuns la incidente**: Elaborarea unui plan detaliat pentru a răspunde rapid și eficient la incidentele legate de deepfake-uri, inclusiv proceduri de comunicare internă și externă.
- **Exerciții de simulare**: Organizarea de exerciții periodice de tip "table top" pentru a testa și îmbunătăți planurile de răspuns la diverse scenarii de deepfake.

[15] Vezi link: Content Authenticity Initiative

6. Colaborare și parteneriate intersectoriale

- **Parteneriate cu alte organizații**: Colaborarea cu alte companii, instituții guvernamentale și organizații non-guvernamentale pentru a împărtăși informații și bune practici privind combaterea deepfake-urilor.
- **Participarea la inițiative comune**: Implicarea în inițiative precum Coalition for Content Provenance and Authenticity (C2PA) sau Project Origin pentru a susține standarde comune de autenticitate a conținutului.

7. Monitorizarea și raportarea amenințărilor,

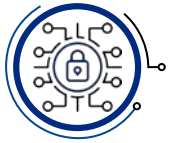
- **Monitorizare continuă**: Utilizarea de instrumente de monitorizare pentru a detecta rapid conținutul fals sau manipulat care ar putea afecta organizația.
- **Canale oficiale de raportare**: Raportarea prin canale dedicate a atacurilor deepfake către instituțiile relevante, precum platforma Ministerului Cercetării, Inovării și Digitalizării #nofake

8. Gestionarea riscurilor și conformitate

- **Evaluarea riscurilor**: Efectuarea de evaluări regulate ale riscurilor asociate deepfake-urilor și actualizarea corespunzătoare a politicilor de securitate.
- **Respectarea reglementărilor**: Asigurarea că organizația respectă toate prevederile legale aplicabile și reglementările relevante privind protecția datelor și combaterea dezinformării.

9. Comunicare transparentă și gestionarea reputației

- **Comunicare proactivă**: În cazul identificării unui deepfake care afectează organizația, se recomandă comunicarea rapidă și transparentă cu publicul pentru a clarifica situația și a minimiza impactul negativ asupra reputației.
- **Strategii de relații publice**: Dezvoltarea strategiilor de relații publice pentru a răspunde eficient la potențialele atacuri de dezinformare și pentru a restabili încrederea publicului.



10. Implementarea politicilor și procedurilor de securitate

- **Politici clar definite**: Stabilirea de politici clare privind utilizarea și distribuirea conținutului media în organizație.
- **Controlul accesului**: Implementarea măsurilor stricte de control al accesului la informațiile sensibile și la resursele media pentru a preveni utilizarea neautorizată.

Implementarea acestor recomandări poate ajuta organizațiile să se protejeze eficient împotriva amenințărilor deepfake, reducând riscurile de securitate, prezervând reputația și asigurând continuitatea operațiunilor. Adaptarea și personalizarea acestor strategii în funcție de specificul fiecărei organizații sunt hotărâtoare pentru o gestionare eficientă a riscurilor asociate deepfake-urilor.

Concluzii

Pe măsură ce tehnologia evoluează, amenințările devin mai sofisticate și greu de detectat, punând în pericol inclusiv sistemele de autentificare biometrică și procesele de luare a deciziilor strategice. Tot mai des, deepfake-urile sunt folosite pentru **uzurparea identității, manipularea informațiilor financiare și atacuri asupra infrastructurilor critice**, ceea ce le conferă un rol central în tacticile de atac cibernetic la nivel global.

Tehnologia deepfake a devenit o problemă emergentă și dificil de gestionat, amenințând **autenticitatea informațiilor, securitatea cibernetică (confidențialitatea, integritatea, disponibilitatea), precum și încrederea publicului sau a partenerilor** în conținutul digital produs sau gestionat de către organizație. Pe măsură ce tehnologiile legate de deepfake devin mai accesibile, atât pentru utilizări legitime, cât și pentru scopuri ilicite, organizațiile trebuie să fie pregătite să gestioneze riscurile implicate. Fără măsuri de prevenție și răspuns adecvate, atacurile deepfake pot **compromite rapid reputația, securitatea datelor și stabilitatea financiară** a unei companii.

Atacurile deepfake nu sunt doar o provocare tehnică, ci și una managerială, care afectează reputația, relațiile comerciale și chiar moralul angajaților. Un atac de acest tip poate distruge rapid ani de muncă și relații construite cu parteneri și clienți.

Este evident că deepfake-urile nu vor dispărea, ci dimpotrivă, vor deveni din ce în ce mai sofisticate și greu de detectat. În acest context, managerii trebuie să-și schimbe modul de gândire – securitatea nu mai este doar o problemă tehnică de IT, ci o prioritate strategică care trebuie integrată în toate aspectele operaționale ale organizației.

Pe scurt, deepfake-urile reprezintă o realitate cu care organizațiile trebuie să se confrunte activ. Managementul riscurilor cibernetice trebuie să fie unul proactiv și nu reactiv, care să ia în considerare riscurile legate de deepfake. Investițiile în tehnologie, educație și procese sunt cheia pentru a naviga cu succes în acest peisaj tot mai complex.

Acest material a fost realizat de următorii experți ai DNSC:

Daniel Abotezătoaei, Dan Andrieș, Mihaela Dan, Alex Leoreanu, Irina Nemoianu, Cristian Nistor, Antonio Radu, Laurențiu Zăbavă, Cezar Bărbuceanu