AIRNITE

ZERO DAY

NÚMERO 19/2026 · IA

El falso director financiero en la videollamada: así robaron los deepfakes 25 millones de dólares

Un empleado de la ingeniería Arup en Hong Kong transfirió unos 25 millones de dólares tras una videollamada con un falso director financiero y falsos compañeros. Cómo funciona el fraude con deepfakes y cómo aconseja protegerse el BSI alemán.

Publicado: 21 de noviembre de 2026 Tiempo de lectura: 5 min Autor: Redacción de Airnite

SOFTWARE. SECURITY. CODE.

// LA SITUACIÓN EN CIFRAS

200 M HK$
importe transferido
unos 25,6 millones de dólares (Fortune)

15+
transferencias
a cinco cuentas bancarias en Hong Kong (Fortune, CFO Dive)

0
sistemas internos comprometidos
según un portavoz de Arup (Fortune)

Formación
contramedida central
concienciar a los afectados según el BSI; la técnica no protege por completo

Una videollamada con el director financiero y varios compañeros, una transacción confidencial, instrucciones claras: para un empleado de la ingeniería británica **Arup** en Hong Kong, todo parecía a principios de 2024 una jornada normal. Al final había transferido unos **25 millones de dólares** a estafadores. Ninguno de sus interlocutores era real.

// ¿Qué ha pasado?

Según Fortune y CFO Dive, que se basan en la policía de Hong Kong y el Financial Times, un empleado recibió un mensaje supuestamente del **director financiero**, con sede en el Reino Unido, sobre una «transacción confidencial». Después participó en una videoconferencia en la que aparecían el director financiero y otros compañeros, todos ellos **deepfakes**. A continuación transfirió en total **200 millones de dólares de Hong Kong**, unos 25,6 millones de dólares estadounidenses, en más de 15 operaciones a cinco cuentas de Hong Kong.

Solo se dio cuenta del fraude al consultar con la sede central. Según CFO Dive, Arup denunció el caso a la policía en enero de 2024; la policía lo hizo público en febrero sin nombrar a la empresa, y en mayo de 2024 se supo que la víctima era Arup. Según Fortune, un portavoz confirmó que se usaron voces e imágenes falsas; **ningún sistema interno resultó comprometido**.

// ¿Cómo funciona el ataque?

El ataque no necesita malware ni intrusión en la red. Ataca a las personas, no a los sistemas. Las herramientas de IA generan, a partir de material público, voces y caras engañosamente reales. Combinadas con la prisa, la confidencialidad y la autoridad de los superiores, crean una situación en la que cuesta hacer preguntas.

El BSI alemán describe justo este escenario como **fraude del CEO**: un atacante llama con la voz clonada de un directivo para provocar una transferencia. Según Fortune, el director de informática de Arup, Rob Greig, dijo que los intentos de fraude contra empresas habían aumentado mucho y que es un asunto de todo el sector, la economía y la sociedad.

// ¿A quién afecta?

Afecta a toda empresa en la que la plantilla pueda ordenar pagos y en la que los directivos aparezcan en público con su imagen y su voz, por ejemplo en vídeos, entrevistas o conferencias. Corren especial riesgo los departamentos financieros, las asistencias de dirección y las filiales en el extranjero, donde la sede central a menudo solo está presente por vídeo.

// ¿Qué hay que hacer ahora?

El BSI señala la **concienciación y la formación** de las personas potencialmente afectadas como medida central. Según el BSI, la detección técnica de deepfakes no es fiable en todas las condiciones y las contramedidas no ofrecen, en general, una protección completa. Por eso los procesos son decisivos: doble control en los pagos, devolución de llamada a números conocidos, preguntas de control y una cultura en la que preguntar al jefe esté permitido y bien visto. La lista de control de abajo resume los pasos.

// ¿Cómo ayuda Airnite?

En la **formación**, Airnite entrena de forma práctica a dirección, finanzas y asistencias para reconocer deepfakes y fraude del CEO. En la **consultoría** revisamos con usted los procesos de autorización de pagos y los canales de comunicación. Con **simulaciones** acordadas dentro de las pruebas de seguridad mostramos dónde siguen siendo vulnerables hoy los procedimientos.

> Nota: los datos del caso Arup proceden de informaciones de prensa; no pudimos consultar directamente una fuente primaria de la policía de Hong Kong ni de Arup. Estado de la investigación: 21 de noviembre de 2026.

Lista de control: qué hacer ahora

[+] Establezca un principio de doble control para pagos inusuales o urgentes que nadie pueda saltarse por teléfono o videollamada.

[+] Haga obligatoria una devolución de llamada a un número conocido y registrado internamente antes de pagar, nunca a los datos de la solicitud.

[+] Acuerde una palabra clave o pregunta de control para las instrucciones confidenciales de la dirección.

[+] Forme de forma específica a dirección, finanzas y asistencias sobre deepfakes y fraude del CEO.

[+] Anime expresamente a la plantilla a comprobar incluso las «órdenes del jefe», sin temor a consecuencias.

[+] Ante la duda, avise de inmediato al banco, a la policía y, internamente, a la dirección por un segundo canal.

Cómo ayuda Airnite

- Formación – Su equipo aprende nuestras herramientas y procesos.
- Consultoría – Una mirada externa sobre sus planes y proyectos.
- Pruebas de penetración y seguridad – Ataques controlados con un informe claro y un plan de medidas.

¿Reconocería su equipo a un jefe falso?

Airnite forma a la dirección, al departamento financiero y a las asistencias en el fraude del CEO con voces y vídeos falsos y revisa con usted los procesos de autorización de pagos. Si lo desea, probamos los procedimientos con simulaciones realistas y acordadas.

Solicitar una primera conversación · Escribir un correo · Por WhatsApp

Contacto

¿Preguntas sobre este artículo? Escríbanos por WhatsApp: +49 174 6834842

Leer en línea: https://airnite.de/es/revista/deepfake-fraude-del-ceo-videollamada/

Fuentes

Cada dato de este artículo se basa en las fuentes indicadas a continuación. Las fuentes primarias están señaladas.

1. **BSI · Deepfakes – Gefahren und Gegenmaßnahmen** · FUENTE PRIMARIA
   Fuente primaria (autoridad): fraude del CEO con voz clonada, contramedidas, límites de la detección
   https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kuenstliche-Intelligenz/Deepfakes/deepfakes_node.html
2. **Fortune · A deepfake 'CFO' tricked the British design firm behind the Sydney Opera House in $25 million scam** · 17/05/2024
   Prensa económica: importe, desarrollo, declaraciones de Arup
   https://fortune.com/europe/2024/05/17/arup-deepfake-fraud-scam-victim-hong-kong-25-million-cfo/
3. **CFO Dive · Scammers siphon $25M from engineering firm Arup via AI deepfake 'CFO'** · 17/05/2024
   Prensa especializada (según el Financial Times): primer contacto, cuentas, cronología
   https://www.cfodive.com/news/deepfake-scam-engineering-firm-arup-25-million-fraud-hong-kong-cfo/716501/

Información editorial general, no constituye asesoramiento jurídico ni una evaluación de sus sistemas concretos. Vigencia: fecha de publicación.

Airnite GmbH · Am Waldbach 7 · 77654 Offenburg · airnite.de