MONITORLEGALE

ULTIME NOTIZIE
TUTTE LE NEWS →

29 Maggio 2026
Orrick e Ropes & Gray nell'acquisizione di Rogelfrut da Arca Space Capital

29 Maggio 2026
Quarta emissione ATI da 500 milioni di BPER Banca. Chiomenti e Clifford Chance advisor

28 Maggio 2026
Green Arrow Capital entra nei data center per la joint venture con Lazzari. Parola Associati e Gitti and Partners advisor

28 Maggio 2026
Rinnovabili: finanziamento di ACL Energy e Qualitas Energy, Bonelli e Gop advisor

1 Giugno 2026

Deepfake e sicurezza aziendale: cresce il rischio di impersonificazione

di Di Luciana Cipolla, partner di La Scala Società tra Avvocati

CONDIVIDI:

La diffusione dei deepfake basati su intelligenza artificiale sta superando la capacità di risposta di molte organizzazioni. Secondo il Deepfake Readiness Benchmark Report di GetReal Security, i tentativi di impersonificazione non riguardano più soltanto casi isolati o scenari sperimentali, ma interessano ormai processi ordinari come selezione del personale, videoconferenze, help desk IT e sistemi di autenticazione biometrica.

Il dato è particolarmente rilevante anche per il mercato assicurativo, chiamato a valutare l'evoluzione del rischio cyber e delle frodi digitali. Il report evidenzia che 8 organizzazioni su 10 hanno già incontrato deepfake o tentativi di impersonificazione almeno occasionalmente, mentre il 45% li rileva con frequenza. Ancora più significativo è il dato relativo alle grandi imprese: il 41% delle organizzazioni con almeno 1.000 dipendenti dichiara di aver assunto o inserito in organico un candidato falso o un impostore.

La minaccia non si concentra su un solo canale. I deepfake possono riguardare voce, video, identità sintetiche, furto di credenziali e accessi fraudolenti ai sistemi aziendali. Questo amplia l'esposizione delle imprese e rende insufficiente un presidio fondato soltanto sulla formazione del personale o su controlli di identità effettuati in un singolo momento.

Per le compagnie assicurative, il fenomeno impone una riflessione sia in fase assuntiva sia nella gestione dei sinistri cyber. La crescente sofisticazione delle tecniche di impersonificazione può incidere sulla valutazione del rischio, sulle misure minime di sicurezza richieste agli assicurati e sull'analisi delle coperture relative a frodi informatiche, ingegneria sociale, accessi non autorizzati e compromissione dell'identità digitale.

Il messaggio operativo è chiaro: le aziende dovranno rafforzare i sistemi di monitoraggio continuo, verifica dell'identità e controllo degli accessi. Per il settore assicurativo, i deepfake rappresentano un fattore di rischio destinato a incidere sempre di più sulla costruzione delle polizze cyber e sulla delimitazione delle garanzie.

#sicurezza #assicurazioni #Milano #cybersecurity #2026 #deepfake
#impersonificazione #biometria #ingegneriasociale #autenticazione

REview Web Edition 30 Maggio - 5 Giugno