Ti fido di te.

Come la supply chain è diventata la backdoor del mondo

ICTFest 2026

Simone Malcangi – Produce ICT s.r.l.

Il numero che cambia tutto

19

secondi

Si è calcolato che, ogni 19 secondi, secondi, nel mondo, un'organizzazione cade vittima di ransomware.

Nel tempo di quest talk:
~100 attacchi. (94,7)

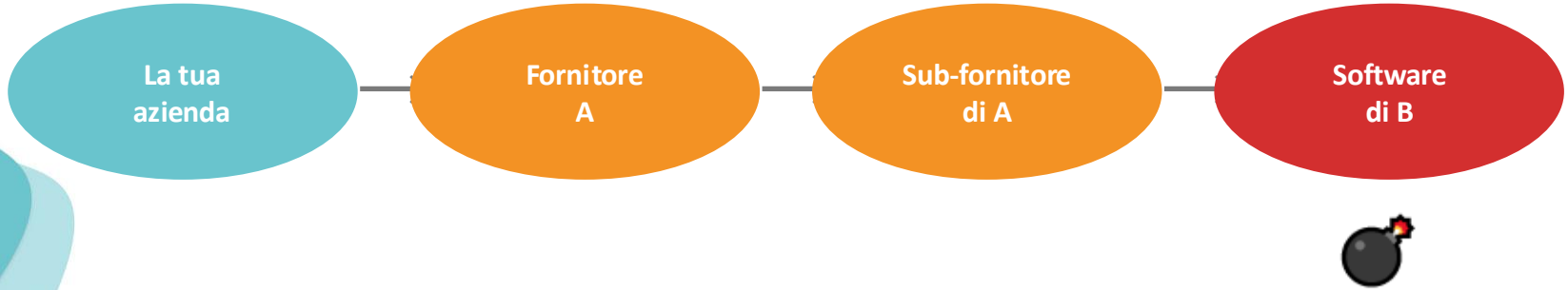
Fonte: CybersecurityNews, 2025

Quanti dei vostri fornitori hanno accesso ai vostri sistemi in questo momento?

Sapete esattamente cosa fanno quando entrano?

Il paradosso della fiducia.

Il tuo livello di sicurezza è esattamente uguale a quello del tuo fornitore più debole.



"Se mi fido di te, e tu ti fidi di lui, allora io mi fido di lui — anche se non lo so."

Il malware arrivato con l'aggiornamento

CASO: SolarWinds / Sunburst — 2020

18.000

organizzazioni colpite

9 mesi

accesso silenzioso

US Gov

tra le vittime

Fonte: NPR Investigation; SolarWinds CEO Statement

SolarWinds — 2020

CASO REALE

Un aggiornamento software firmato digitalmente.
Considerato sicuro. Distribuito a 18.000 organizzazioni.
Conteneva un malware silente da 9 mesi.

18.000

organizzazioni infettate,
inclusi enti governativi USA

9 mesi

accesso non rilevato
marzo–dicembre 2020

Mar. 2020

data inizio infezione,
scoperta solo a dicembre

NPR Investigation – SolarWinds Hack · npr.org/2021/04/16/985439655

La password del server di produzione.

Fonte: ricercatore di sicurezza Vinoth Kumar, via Bloomberg News (riportato da NPR, Dic 2020)

Non incidenti isolati. Un metodo che si ripete. ripete.

"Il prossimo è già in corso. Da qualche parte."

NotPetya: White House assessment ($10B) · SolarWinds: CISA Alert AA20-352A · Kaseya/MOVEit: CISA advisories

Colonial Pipeline — Maggio 2021

Più grande attacco ransomware a infrastruttura energetica USA.

Come sono entrati:

Password compromessa di un account VPN inattivo, SENZA autenticazione a due fattori.

Impatto:

6 giorni di pipeline ferma. 45% del carburante East Coast USA bloccato. Dichiarato stato d'emergenza.

$4,4M

riscatto pagato in Bitcoin a DarkSide.
"Era la cosa giusta da fare per il paese."
— CEO Joseph Blount, WSJ, 19 maggio 2021

Wikipedia – Colonial Pipeline ransomware attack · en.wikipedia.org/wiki/Colonial_Pipeline_ransomware_attack · Huntress Threat Library · huntress.com/threat-library/ransomware/colonial-pipeline-ransomware

Colonial Pipeline — 2021

Più grande attacco a infrastruttura petrolifera degli Stati Uniti.

$4,4M	riscatto pagato in Bitcoin
6 giorni giorni	pipeline completamente ferma
1 password	VPN senza MFA — vettore iniziale

La vulnerabilità:

Account VPN inattivo senza MFA abilitata.

La lezione:

Non è un problema IT.
È business continuity
— e sicurezza nazionale.

"Pagare il riscatto è stato il male minore."

Fonte: Wikipedia; Georgetown Law Review; Wired

NotPetya — Giugno 2017

Non era ransomware. Era un'arma. Iniziò come aggiornamento del software contabile ucraino M.E.Doc.

~$10B

danni stimati totali
(White House assessment, 2018)

Maersk	$250–300M	45.000 PC reinstallati in 10 giorni
Merck	$870M	produzione farmaci ferma
FedEx/TNT	$400M	sistemi logistics distrutti
Mondelēz	$188M	supply chain alimentare bloccata

"Non erano target. Erano danni collaterali. Ma pagarono comunque."

Ransomware-as-a-Service: il cybercrime è una franchise.

Non un hacker solitario. Un'industria organizzata con ruoli, KPI e percentuali sulle vendite.

Developer

Scrive e mantiene il malware. Lo affitta agli affiliati.

Affiliato

Paga per accedere al toolkit. Sceglie i target.

Attacco

Phishing, RDP esposto, supply chain.

Riscatto

Richiesta in criptovaluta. Doppia estorsione.

Split

20–30% al developer. Il resto all'affiliato.

64 gruppi RaaS attivi nel 2025 con programmi di affiliazione formalizzati.

ARUP — Londra, 2024

$25.000.000

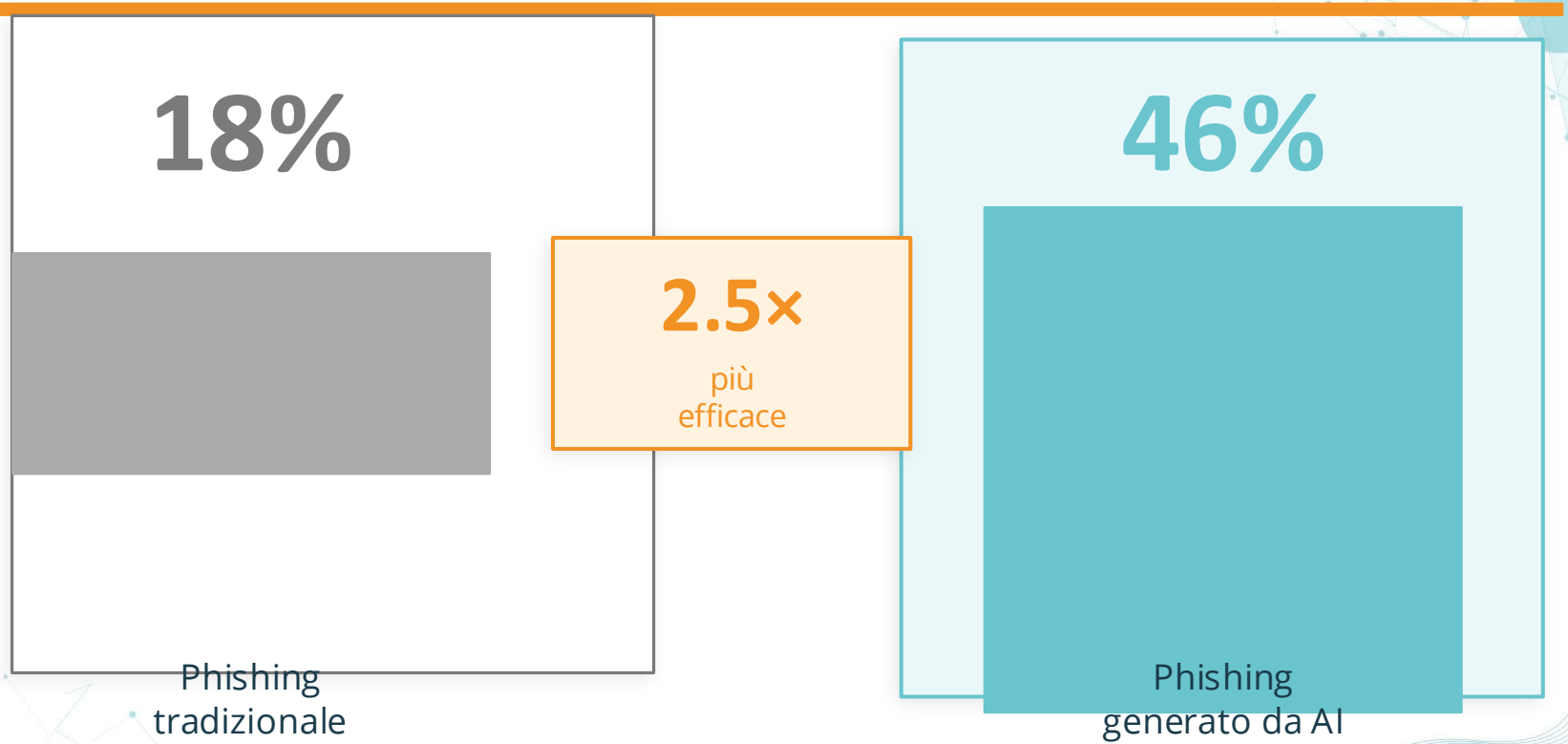
sottratti con una videochiamata deepfake del CFO. L'impiegato ha autorizzato il bonifico.

Come ha funzionato:

1. AI ha clonato voce e volto del CFO da materiale pubblico
2. Ha simulato una videochiamata di gruppo con più partecipanti
3. Il dipendente ha trasferito il denaro in più tranche

Reuters, 5 Feb 2024 · reuters.com/technology/deepfake-video-call-scam-hong-kong-2024 · WEF Cybersecurity Outlook 2025

Il phishing generato da AI è 2,5× più efficace.



La difesa più efficace esiste già.

99%

degli attacchi basati
su credenziali compromesse
blocca l'MFA.

"Il problema non è la tecnologia. È adottarla."

Microsoft Digital Defense Report 2024 - microsoft.com/en-us/security/blog/2024/10/15/microsoft-digital-defense-report-2024

Il paradosso dell'AI nel 2025.

Stiamo adottando l'AI più velocemente di quanto capiamo i rischi.

66%

delle organizzazioni ritiene l'AI la principale minaccia cybersecurity 2025

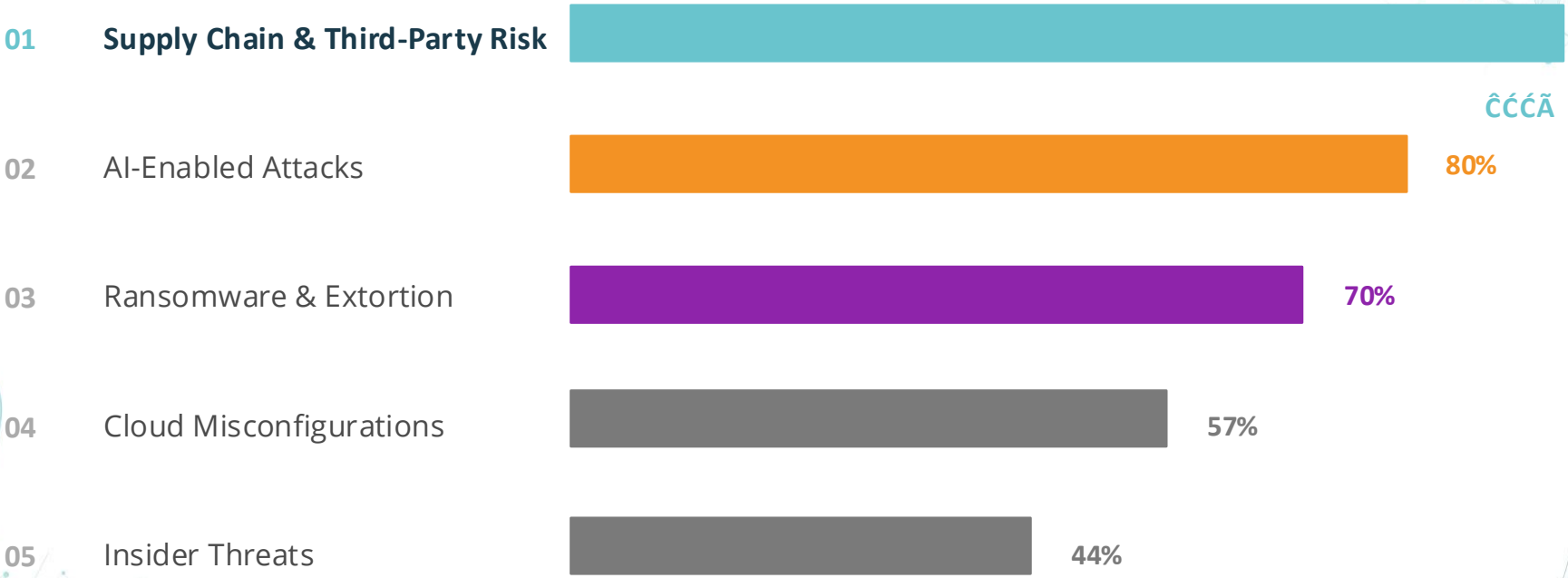
vs

37%

ha processi in atto per valutare la sicurezza degli strumenti AI adottati

WEF Press Release, 13 Jan 2025 · weforum.org/press/2025/01/global-cybersecurity-outlook-2025

La supply chain è il problema #1.



Il 54% delle grandi organizzazioni identifica la supply chain come il principale ostacolo alla cyber resilienza.

3 azioni concrete da fare domani mattina.

01

Mappa la supply chain digitale

Censisci tutti i fornitori con accesso ai sistemi. Chi entra? Con quali privilegi? Con quale frequenza viene verificato?

Se non hai la risposta in 30 secondi → problema.

02

Zero Trust al vending

Nessuna fiducia di default verso i fornitori. Separazione accessi, minimo privilegio, audit regolari ogni trimestre.

Non è burocrazia — è sopravvivenza.

03

Tabletop sul fornitore più critico

Simula: il tuo MSP viene compromesso. I tuoi sistemi sono ancora isolati? Il piano di risposta tiene?

Lo scoprirai solo provando.

"Non serve un budget enorme. Serve una decisione."

Chi ha le chiavi di casa tua in questo momento?

Non è una domanda retorica.
Pensaci e rispondi entro 48 ore.

Media dwell time di un APT prima del rilevamento: 197 giorni · IBM Cost of a Data Breach Report 2024

Fonti e riferimenti.

→ WEF Global Cybersecurity Outlook 2025 (Accenture, gen. 2025)
weforum.org/publications/global-cybersecurity-outlook-2025

→ WEF Press Release — GCO 2025 key statistics
weforum.org/press/2025/01/global-cybersecurity-outlook-2025

→ NotPetya — Columbia SIPA Case Study
sipa.columbia.edu/sites/default/files/2022-11/NotPetya%20Final.pdf

→ NotPetya — Control Engineering / Maersk analysis
controleng.com/throwback-attack-how-notpetya-accidentally-took-down-global-shipping-giant-maersk

→ Colonial Pipeline — Wikipedia
en.wikipedia.org/wiki/Colonial_Pipeline_ransomware_attack

→ Colonial Pipeline — Huntress Threat Library
huntress.com/threat-library/ransomware/colonial-pipeline-ransomware

→ SolarWinds / SUNBURST — NPR Investigation
npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack

→ ARUP deepfake scam $25M — Reuters
reuters.com/technology/deepfake-video-call-scam-hong-kong-2024-02-05

→ Microsoft Digital Defense Report 2024
microsoft.com/en-us/security/blog/2024/10/15/microsoft-digital-defense-report-2024

→ Microminder Cybersecurity Statistics 2025
microminder.com/blog/cybersecurity-statistics-2025

→ IBM Cost of a Data Breach Report 2024
ibm.com/reports/data-breach

Quesiti & Aneddoti:
che Vi viene a mente con questi link ??

Claude Glasswing:
https://www.difesaonline.it/2026/04/10/project-glasswing-vulnerabilita-zero-day-sistemi-operativi-browser/
Fuga sorgente Claude:
https://www.ilsole24ore.com/art/anthropic-mette-nudo-claude-codice-finisce-online-un-errore-umano-AI4PQzHC
Hacking Team Hacked:
https://www.theguardian.com/technology/2015/jul/06/hacking-team-hacked-firm-sold-spying-tools-to-repressive-regimes-documents-claim

Contatti:
Simone Malcangi
ictfest2026@produceict.it

ICTfest

"La fiducia si guadagna. Non si eredita."

Nel mondo in cui viviamo, la fiducia deve essere guadagnata — non data per scontata, e mai delegata.
Grazie per l'opportunità e per l'attenzione

ICTFest 2026 · Ti fido di te.