Search And Agents Are One Product. You Only Need One Playbook via @sejournal, @slobodanmanic

Google Search is becoming an agent manager. Sundar Pichai said it plainly across two interviews this spring:

> *“A lot of what are information-seeking queries will be agentic in Search. You’ll be completing tasks. You’ll have many threads running.”*

One week later, at Google Marketing Live 2026, Nick Fox, the SVP who oversees Search, Ads, and Commerce, said the corollary:

> *“The way to optimize for AI search is the same way to optimize for search. Create great content.”*

When the CEO describes a product direction and the SVP confirms the optimization path, treating search and agents as two separate disciplines means running two playbooks for one product.

That surface is already live. AI Mode is in the Chrome address bar. Search agents run in the background on queries too long for a single click. Chrome auto-browse fills forms and completes bookings on behalf of users with OS-level permissions. These are not separate products with separate optimization playbooks. They all inherit the same web.

What Pichai Actually Said

Pichai gave two interviews this spring that together draw the clearest picture of where Google Search is headed. On the Cheeky Pint podcast in April 2026, he described the trajectory: “If I fast-forward, a lot of what are just information-seeking queries will be agentic in Search. You’ll be completing tasks. You’ll have many threads running.” He called it “Search as an agent manager” and framed it as already happening in AI Mode, where users run deep research queries that do not fit the classical keyword model.

Then, on Decoder with Nilay Patel after I/O 2026, he did something more revealing. Patel showed him a live AI Overview result on his phone for “best Chromebook.” Pichai looked at it and said: “It’s probably more opinionated than it should be for the particular query you showed me.”

That admission matters more than the convergence statement. He is not pretending the product is finished. He called it scope for improvement in a fast-evolving space. In the same interview, he also said Google is committed to sending traffic to the web: “Everything we do across all, you will see us five years from now sending a lot of traffic out to the web. I think that’s the product direction we are committed to.”

Both claims sit next to each other in the same interviews. The product direction is convergence: search queries become agentic, tasks get completed inside Search, agents browse on behalf of users. The promise is continuity: traffic will still flow to websites. Hold both in your head at the same time, because that gap between the direction and the promise is where your risk lives.

Nick Fox Said The Same Thing From A

Different Angle

At Google Marketing Live 2026, Nick Fox sat down with Semafor’s Ben Smith and addressed the optimization question directly. Fox is Google’s SVP of Knowledge and Information, the person who oversees Search, Ads, and Commerce. His statement: “The way to optimize for AI search is the same way to optimize for search. Create great content.”

He added one qualifier: “Go beyond the surface level.” His reasoning is that AI handles first-level responses, so the content that performs in AI search is content that goes deeper than the summary the model already produces. “If you’re looking to buy something, you don’t want to hear what the AI says. You want to hear someone that’s used it.” This is the commodity-vs-non-commodity content distinction Google has been circling for a while now: if the AI can produce the answer itself, your content needs to offer something the AI cannot.

This is also what No Hacks guest Jono Alderson has been saying for over a year. The content that AI ignores is the content that restates what the model already knows. The content that gets cited is the content that carries something the model has to retrieve because it cannot generate it: original data, first-person experience, named-entity specificity, a take the model is not confident enough to produce on its own.

When the CEO says the products are merging and the SVP says the optimization is the same, the implication lands: one strategy, not two. The separate “AEO strategy” or “GEO strategy” that consultants have been selling as a new discipline collapses when the vendor itself says it is one playbook. The r/TechSEO community arrived at the same conclusion this week when Google published its official AI optimization guide: “It’s basically just. SEO.”

What This Means For The Website You Are Building

The website that works for classical search is the same website that works for agents. Server-rendered HTML so the content is visible without JavaScript hydration. A study I published this week measured 274 fintech companies and found 36% are partially invisible to AI crawlers because they depend on JavaScript to render core content. 17% deliver zero content without JS execution. The fix is not complicated. 99% of those same websites deliver full content once rendered. The gap is the default: raw HTML first, not JS-rendered-eventually. Semantic markup so the agent knows what each element is. Structured data so the identity is machine-readable. Fast delivery so neither the crawler nor the agent times out. Internal linking so both the index and the agent can navigate the full surface.

None of this is new. They are the same requirements Google published in its agent-friendly checklist in April, and they map directly to what AI agents read when they visit your website: the accessibility tree, the semantic structure, the extractable content.

The companies that treated agent-readiness and search optimization as the same discipline were accurate. They were not early. The vendor confirmed what the practice already showed: the audit is the same audit applied to a visitor class that now includes both humans on Google Search and agents in AI Mode.
Build for one playbook: machine-readable identity, extractable content, discoverable actions, server-rendered and semantic and structured and fast and well-linked. That description fits classical search and the agentic web and the product Pichai is describing, which is both at once.

Pichai admitted the product is not finished. “More opinionated

than it should be” is a refreshingly honest read of a product in motion. The gap between where AI Overviews are today and where search-as-agent-manager is going is your window. The direction is set. Build for one playbook now, and you are building for the product Google is becoming.

More Resources:

This post was originally published on No Hacks.

Featured Image: Meepian Graphic/Shutterstock

https://www.searchenginejournal.com/search-and-agents-are-one-product-you-only-need-one-playbook/576191/

Google Says AI Visibility Hinges On Content People Actually Want To Read via @sejournal, @martinibuster

Google’s VP of Search, Liz Reid, sat down for an interview where she talked about the relationship between Google and publishers. When asked what the new rules are for showing up in AI search, she said that publishers need to publish content that people actually want to read.

Google Says Publisher Traffic Loss Is Not Just AI

One of the points that Reid stressed is that publisher traffic loss is not just about AI. She put part of the blame on people seeking out non-textual content. Her answer was in the context of what she would "say to publishers about the reality of this new time."

Reid answered:

> *"I think to start with, there are, first of all, multiple things going on besides AI, right? One of the things that we see is that people are often going for new formats, right? They want to see videos, not just text. They're often going to social media for content.*
>
> *There was a recent study from Reuters around this, really just talking about how people are shifting, and so one of the things I would generally tell publishers is make sure you're innovating with what users want and how they want, right?"*

Google Says Publishers Must Make Content People Want To Read

The next part of her answer to the question of what publishers need to know about the "reality of this new time" is that if publishers want to be seen on AI search, they need to not make the kind of slop content that is the "1,000th copy" of everything else. She put the burden on publishers to step up and make better content that people actually want to read.

She explained:

> *"I think the second thing that is really important is that people, to the extent that you produce really interesting*

expertise content, we still see that people are interested in that, right?

…And so the more that publishers produce content that is really where they shine, what they bring to the table, that it's unique, it's not the 1000th copy of the same story, but it's something that has an interesting take on it. The more I think we'll see that people will continue to click through and read that."

What Publishers Can Do To Be More Visible In AI

The interview hosts circled back to what publishers can do to make content more visible in AI. They tried to elicit an answer that addressed the "new direction" that AI search is headed in, noting that publishers are concerned.

They asked:

"What can, what can publishers do or creators do to make their content more visible to AI? If this is something, if this is kind of the new direction that all of this is headed, which it clearly is, and publishers are concerned about getting the right eyeballs on their content.

How can they work with the system to ensure that they're kind of playing by the new set of rules and getting their content maximized in front of the right places at the right time?"

Liz Reid answered that the way to be seen is to make content that people want to read.

She explained:

"Yeah, I mean, I think I would probably put it in two buckets. The first is make sure we can access your content.

> *Like if you block the content, that will not work. If it makes it hard to discover, then that's difficult. We have various tools in webmaster console that give you controls so that publishers can choose. But making it easier for us to access is certainly the first step.*
>
> *But we've also published an updated set of guidelines around for website owners and publishers to think about how they make great content in this day. At the heart of it is really this continuation of, if you want people to click through, then implicit in there is you want people to read your content.*
>
> *That means you need to make content that people want to read, right? So the more you build the content that your audience will love, the more it will work. The more you build content that you think is just designed for the search engine, but not for the audience, then people will learn that over time.*
>
> *So the more it brings in your expertise, that is sort of fresh and relevant content of what people are curious about, that it brings in that sort of experience, that detail and richness, that's really great."*

Takeaways

Liz Reid's comments show that Google is increasingly viewing publisher success in AI Search as dependent on two conditions:

1. Let Google crawl everything.
2. Create content that people actually want to read.

That kind of approach ignores the Google Zero fears that haunt even big-brand sites that are experiencing declines in search referrals. If the big-brand sites are having a freakout about declining search referrals, where does that leave small-brand publishers who write recipe blogs, product reviews, travel guides, advice, and news?

Watch the interview at about the 18 minute mark:

[embedded content]

Featured Image by Shutterstock/Roman Samborskyi

https://www.searchenginejournal.com/google-says-make-content-people-want-to-read/580642/

New York apre le piscine, il sindaco Mamdani si tuffa in giacca e cravatta

(Adnkronos) – Il sindaco di New York si tuffa in piscina. Vestito con giacca e cravatta. Zohran Mamdani, il primo cittadino della Grande Mela, ha scelto un modo particolare per inaugurare la stagione delle piscine all'aperto in città. L'exploit di Mamdani non è ovviamente passato inosservato. In completo grigio, il sindaco si è posizionato 'ai blocchi di partenza': tuffo apprezzabile e via con qualche bracciata a stile libero, impresa non trascurabile considerata la zavorra dell'abito.

"Mi avevano detto di vestirmi così…", la spiegazione ironica del sindaco, invitato a presentarsi in piscina con un 'suit': la parola, in inglese, indica sia il costume da piscina che il completo. E Mamdani ha scelto la seconda opzione…

–

internazionale/esteri

webinfo@adnkronos.com (Web Info)

Novità su Google, per aggiungere Key4Biz tra le tue fonti preferite, clicca qui

Leggi le altre notizie sull’home page di Key4biz

https://www.key4biz.it/new-york-apre-le-piscine-il-sindaco-mamdani-si-tuffa-in-giacca-e-cravatta/577792/

Europa nella morsa del caldo, in Francia circa mille morti in più rispetto alla norma. In Germania la notte più calda di sempre

(Adnkronos) – Europa nella morsa del caldo. In Francia, da mercoledì scorso, da quando è iniziato il caldo record, si contano circa mille decessi in più rispetto alla media. Lo conferma Santé publique France (SpF), dopo il caldo estremo che ha colpito il Vecchio Continente. “Dal 24 giugno si sono registrati circa mille decessi in più rispetto ai mesi precedenti, secondo dati non ancora definitivi”, hanno reso

noto.

Si tratta per lo più di over 65 e viene segnalato anche un aumento del 40% dei casi di decesso in casa. “Più di 1.200 decessi, per diverse cause, sono stati registrati il 24 giugno e oltre 1.400 decessi al giorno si sono contati il 25 e il 26 giugno – spiegano – A titolo di confronto, si contavano tra i 900 e i 1.000 decessi al giorno ad aprile, maggio”. Così in totale, da mercoledì, si contano circa un migliaio di decessi in più rispetto alla media, anche se non si tratta di casi ufficialmente attribuibili al caldo record. L’aumento dei decessi riguarda “tutte le fasce di età” e gli “effetti” del caldo estremo “possono colpire tutta la popolazione”, ricordano da SpF, precisando come “tuttavia l’85% dei decessi osservati riguardi persone di 65 anni o più grandi”.

In Germania è stata la notte più calda di sempre. Nelle ore notture le temperature hanno raggiunto i 29,4 gradi, ha reso noto il servizio meteorologico tedesco (Dwd). Secondo i dati ancora provvisori, il record è stato registrato a Kubschütz, comune della Sassonia.

Nella giornata di ieri nel Paese sono state registrate nuove temperature da primato, con un picco di 41.5 gradi rilevato a Möckern, nella zona di Drewitz. Caldo estremo anche in Danimarca, dove l’istituto di meteorologia ha reso noto di aver registrato la temperatura più alta di sempre. “Abbiamo avuto la giornata più calda in assoluto dall’inizio del monitoraggio nel 1874”, si legge in un post su X. Sono stati inizialmente segnalati i 36.6 gradi registrati a nord di Odense, un “record” presto battuto dai 37 gradi rilevati a Ødum, a nord di Aarhus.

In Spagna si stima che la ondata di calore abbia causato oltre 200 morti in quattro giorni. Anche in altri Paesi europei come l’Austria, il Belgio e la Svizzera si stanno registrando temperature estreme e un aumento dei decessi.

In Italia prosegue il weekend torrido, con allerta caldo massima in 18 città anche oggi. Stando all’ultimo aggiornamento del bollettino sulle ondate di calore del ministero della Salute, oltre ai 18 capoluoghi bollino rosso (livello 3, indice di “condizioni di emergenza, con possibili effetti negativi sulla salute di persone sane e attive e non solo sui sottogruppi a rischio come gli anziani, i bambini molto piccoli e le persone affette da malattie croniche”), si contano anche 6 città con bollino arancione (livello 2, segno di “condizioni meteo che possono rappresentare un rischio per la salute, in particolare nei sottogruppi di popolazione più suscettibili”).

–

internazionale/esteri

webinfo@adnkronos.com (Web Info)

Novità su Google, per aggiungere Key4Biz tra le tue fonti preferite, clicca qui

Leggi le altre notizie sull’home page di Key4biz

https://www.key4biz.it/europa-nella-morsa-del-caldo-in-francia-circa-mille-morti-in-piu-rispetto-alla-norma-in-germania-la-notte-piu-calda-di-sempre/577784/

Iran, nuovi raid Usa e tregua in bilico. Teheran: “Determinati a difenderci da aggressione” – Diretta

(Adnkronos) –
Tregua tra Iran e Stati Uniti in bilico. Donald Trump ha confermato che le forze Usa hanno attaccato “depositi di missili e droni” e altri siti in Iran e ha minacciato di “concludere” con la forza “militare il lavoro iniziato”. “Velivoli Usa hanno attaccato siti iraniani usati come depositi di missili e droni, radar costieri, per aver violato ancora una volta l’accordo di cessate il fuoco!”, ha scritto il presidente Usa su Truth nelle ultime ore accusando Teheran di aver violato il cessate il fuoco. E ha alzato i toni con un monito in cui ha affermato che “potrebbe arrivare un momento in cui potremmo non essere più in grado di essere razionali e trovarci costretti a concludere” con la forza “militare il lavoro che abbiamo iniziato con tanto successo. Se accadesse, la Repubblica islamica dell’Iran smetterebbe di esistere”.

L’Iran ha lanciato missili e droni contro Kuwait e Bahrein in risposta ai massicci raid americani che poche ore prima avevano colpito almeno dieci obiettivi militari e diverse località nell’area dello Stretto di Hormuz. E afferma di essere “determinato a difendere” la sua “sovranità”. La Repubblica islamica “condanna con forza i raid aerei effettuati alle prime ore di domenica dall’esercito terroristico americano contro vari siti di sorveglianza e monitoraggio lungo la costa meridionale del Paese”. Una nota del ministero degli Esteri insiste sulla “determinazione a

difendere la sovranità nazionale dell’Iran” di fronte all’ “aggressione” americana.

Le ultime notizie di oggi domenica 28 giugno in diretta sul conflitto.

–

internazionale/esteri

webinfo@adnkronos.com (Web Info)

Novità su Google, per aggiungere Key4Biz tra le tue fonti preferite, clicca qui

Leggi le altre notizie sull’home page di Key4biz

https://www.key4biz.it/iran-nuovi-raid-usa-e-tregua-in-bilico-teheran-determinati-a-difenderci-da-aggressione-diretta/577776/

Rinnovo CCNL, turni di notte

e straordinari: i chiarimenti sui bonus in busta paga nel 2026

(Adnkronos) – Arrivano nuove istruzioni operative sulla tassazione di favore introdotta dalla Legge di Bilancio 2026 per le buste paga dei dipendenti.

Come si applica la nuova flat tax del 5 per cento sui rinnovi contrattuali e quella al 15 per cento sulle maggiorazioni per lavoro notturno, festivo e a turni?

Nella circolare pubblicata dall'Agenzia sono dettagaliati i requisiti necessari per la fruizione e i criteri di applicazione delle novità.

Indicazioni anche per chi rientra in Italia fruendo dei regimi speciali di detassazione del reddito.

Gli incrementi retributivi, pagati quest'anno, che derivano dai rinnovi contrattuali firmati nel triennio 2024-2026 beneficiano quindi della tassa piatta anche se relativi ad annualità precedenti.

Questo uno dei principali chiarimenti forniti dall'Agenzia delle Entrate. In pratica il nuovo bonus sugli incrementi retributivi, che prevede un'imposta agevolata, si applica anche agli arretrati, cioè alle somme relative alle annualità precedenti.

L'agevolazione spetta ai dipendenti privati con reddito fino a 33.000 euro lordi: per loro gli incrementi retributivi che derivano dai rinnovi contrattuali, firmati nel triennio 2024-2026 e pagati quest'anno, beneficiano di una flat tax al 5 per cento.

Il bonus in busta paga spetta anche per le somme relative alle

annualità precedenti. Sono comprese anche le somme pagate in relazione alla retribuzione dei giorni di ferie, festività soppresse e permessi, mentre restano esclusi gli importi erogati “una tantum”.

Sempre la Legge di Bilancio 2026 ha introdotto, a beneficio dei lavoratori che hanno un reddito fino 40.000 euro, un’altra forma di tassazione agevolata: una flat tax al 15 per cento per le maggiorazioni e le indennità derivanti da lavoro notturno, festivo, nei giorni di riposo settimanale e per le indennità di turno erogate nel 2026, entro il limite annuo complessivo di 1.500 euro.

Con la
nuova circolare
, l’Agenzia ha sciolto un dubbio frequente per quanto riguarda la maggiorazione riconosciuta in caso di lavoro domenicale e riposo settimanale fissato in un giorno diverso della settimana.

Ebbene, dato che tutte le domeniche sono considerate festivi per legge, la maggiorazione prevista dal CCNL è sempre agevolabile.

Il bonus è, invece, parziale per chi svolge part-time verticale, dove i giorni non lavorati nella settimana sono fisiologicamente più di uno.

Infine, un importante chiarimento riguarda chi rientra in Italia beneficiando dei regimi speciali di detassazione del reddito.

L’Agenzia ha precisato che gli incrementi e le maggiorazioni devono essere assoggettati alle imposte sostitutive (del 5 per cento o del 15 per cento) per l’intero ammontare, senza applicare le riduzioni percentuali dell’imponibile previste per gli impatriati.

—

economia/fisco

webinfo@adnkronos.com (Web Info)

Novità su Google, per aggiungere Key4Biz tra le tue fonti preferite, clicca qui

Leggi le altre notizie sull’home page di Key4biz

https://www.key4biz.it/rinnovo-ccnl-turni-di-notte-e-straordinari-i-chiarimenti-sui-bonus-in-busta-paga-nel-2026/577778/

Caricabatteria attaccato alla presa senza telefono, consuma? Cosa succede

(Adnkronos) – Lasciare il caricabatteria attaccato alla presa, anche senza smartphone, è un’abitudine di molti. Si pensa infatti che, non essendoci collegato nessun dispositivo, non consuma energia. Ma è davvero così? In realtà quando si stacca il dispositivo ricaricato dal cavo di alimentazione il caricabatterie continua a consumare energia elettrica, seppure in modo ridotto. Ma a quanto ammonta questo consumo?

Un caricatore nella presa elettrica senza dispositivo collegato consuma comunque una certa quantità di elettricità. Questo succede perché gli apparecchi dispongono al loro interno di un trasformatore, un componente fondamentale per la ricarica di device elettronici come smartphone, PC, tablet, ma che consuma energia anche quando non sta ricaricando nessun dispositivo se rimane attaccato alla presa. E anche anche se il consumo giornaliero può essere irrisorio, nell'arco dell'anno o di più anni potrebbe incidere sulla spesa.

Un caricatore tradizionale a filo posto in standby consuma mediamente circa 0,2-0,25 W,. Quindi, lasciando il caricabatterie sempre collegato durante tutto l'anno, per un totale di 8.760 ore, i consumi in termini energetici sarebbero di almeno 1.752 Wh.

Bisogna tenere conto inoltre del numero di dispositivi elettrici ed elettronici che si ricaricano in una casa, dall'aspirapolvere a batteria al computer, dal tablet agli smartwatch, e moltiplicare i costi.

Ma la spesa non è l'unico motivo per cui staccare il caricabatteria dalla presa una volta caricato lo smartphone. Bisogna infatti considerare anche i rischi per la sicurezza, visto che un caricabatterie sempre collegato alla presa di corrente può surriscaldarsi, causando problemi al funzionamento del dispositivo e aumentare il rischio di incidenti ed esplosioni. Specialmente se si usano dispositivi privi di controllo e di certificazione che non rispettano le normative Ue, può generare cortocircuiti e innescare incendi.

Inoltre, visti quanti sono gli smartphoneutilizzati nel mondo così come altri device, se tutti avessero questa abitudine, si rischierebbe di consumare inutilmente una grande mole di energia.

—

economia

webinfo@adnkronos.com (Web Info)

Novità su Google, per aggiungere Key4Biz tra le tue fonti preferite, clicca qui

Leggi le altre notizie sull’home page di Key4biz

https://www.key4biz.it/caricabatteria-attaccato-alla-presa-senza-telefono-consuma-cosa-succede/577780/

Rottamazione quinquies: online le comunicazioni AdER. Prima scadenza il 31 luglio 2026

(Adnkronos) – La fase operativa della rottamazione quinquies entra nel vivo.

A partire dal 23 giugno 2026, l’Agenzia delle Entrate-Riscossione (AdER) ha reso disponibile, con leggero anticipo rispetto alla scadenza prevista entro fine mese, la comunicazione delle somme dovute.

Questo documento rappresenta il prospetto ufficiale che definisce il conto complessivo e contiene i bollettini necessari per i versamenti agevolati.

Possono accedere a tali informazioni tutti i contribuenti che hanno presentato istanza di adesione entro il termine del 30 aprile 2026.

La disponibilità online della documentazione permette ai contribuenti di conoscere l'ammontare esatto della definizione agevolata e di pianificare le scadenze relative alle rate concesse.

L'intero set dei documenti relativi alla rottamazione quinquies è consultabile in modalità telematica.

Le modalità di ricezione variano in base alla modalità con cui è stata presentata l'istanza.

In caso di invio tramite l'area riservata del portale AdER, il documento è disponibile all'interno del proprio profilo personale sul sito dell'Agenzia.

Per coloro che hanno inoltrato la domanda tramite l'area pubblica del sito (senza autenticazione), la comunicazione viene inviata via PEC o tramite lettera raccomandata al domicilio fiscale dichiarato nella domanda.

Il documento fornisce un quadro chiaro dei benefici ottenuti, indicando il totale dovuto al netto di sanzioni e interessi, nonché il piano di rateazione.

È opportuno ricordare che, sebbene in fase di domanda fosse possibile scegliere tra il pagamento in un'unica soluzione o il numero massimo di rate, spetta all'AdER definire la ripartizione finale, nel rispetto del vincolo dell'importo minimo di 100 euro per ciascuna rata.

L'Agenzia delle Entrate-Riscossione ha differenziato le comunicazioni in cinque tipologie, contraddistinte da codici

specifici, che chiariscono l’esito della richiesta:

● AT (Accoglimento totale): tutti i debiti inseriti nella domanda sono definibili. La lettera indica l’importo totale dovuto.

● AP (Accoglimento parziale): solo una parte dei debiti è definibile. Il prospetto indica l’importo dovuto per la parte agevolabile e specifica gli importi e le motivazioni di esclusione per i debiti non rientranti nella misura.

● AD (Accoglimento totale, importo zero): i debiti sono tutti definibili, ma non vi sono somme da versare.

● AX (Accoglimento parziale, importo zero): parte dei debiti è definibile ma a costo zero; per la parte non definibile, sono indicate le motivazioni di esclusione e gli importi residui.

● RI (Rigetto): nessuno dei debiti inseriti è definibile. La comunicazione riporta le motivazioni dettagliate del rigetto dell’istanza.

Insieme alla comunicazione, il contribuente troverà i moduli di pagamento (bollettini) relativi alle prime dieci rate.

Per quanto riguarda le quote successive, i moduli di versamento verranno messi a disposizione nell’area riservata del portale AdER. Per chi ha utilizzato l’area pubblica per la presentazione dell’istanza, i bollettini saranno inviati al domicilio indicato prima della scadenza dell’undicesima rata.

Il primo appuntamento da annotare in calendario è fissato per il 31 luglio 2026.

Vale la pena ricordare che la Rottamazione-quinquies perde di efficacia in caso di mancato o insufficiente versamento di due rate, anche non consecutive.

Una regola specifica riguarda i ritardi nei pagamenti. È prevista una tolleranza di

cinque giorni
(pagamento considerato tempestivo se effettuato entro il 5 agosto 2026) esclusivamente per chi ha optato per il pagamento in un’unica soluzione e per l’ultima rata del piano di rateazione.

Al di fuori di queste due casistiche, la regola della tolleranza non si applica ai pagamenti rateali intermedi. È quindi fondamentale prestare massima attenzione al rispetto delle scadenze per non decadere dalla definizione agevolata.

—

economia/fisco

webinfo@adnkronos.com (Web Info)

Novità su Google, per aggiungere Key4Biz tra le tue fonti preferite, clicca qui

Leggi le altre notizie sull’home page di Key4biz

https://www.key4biz.it/rottamazione-quinquies-online-le-comunicazioni-ader-prima-scadenza-il-31-luglio-2026/577782/

Terremoto in Venezuela, ritrovato vivo un bambino di 11 anni

(Adnkronos) – “Pochi minuti fa è stato tratto in salvo, vivo, un bambino di 11 anni a Caraballeda”, nel nord del Venezuela. Ad annunciarlo oggi domenica 28 giugno – con un post su X – la presidente ad interim del Venezuela, Delcy Rodriguez, dopo il devastante terremoto che ha colpito il Paese mercoledì 24 giugno. “In queste ore, ogni vita è motivo di speranza per il Venezuela”, ha aggiunto.

A oltre 70 ore dalle scosse di magnitudo 7.2 e 7.5 l’ultimo bilancio è di 1.430 morti, 3.238 i feriti, 50mila dispersi e 3.142 le famiglie rimaste senza casa.

Da mercoledì sono state almeno 430 le scosse di assestamento. Altre due scosse forti, di magnitudo 4.9 e 4.8, sono state registrate ssbato al largo delle coste del Venezuela, secondo quanto riferisce l’United States Geological Survey. La scossa, riporta il sito del New York Times, è stata avvertita a Caracas dove case e palazzi hanno tremato.

Le operazioni di soccorso procedono tra enormi difficoltà, nel Paese devastato arrivano aiuti da numerosi Paesi, Italia compresa. In molte aree, le operazioni procedono a rilento e la popolazione lamenta la carenza di interventi e coordinamento. A La Guaira, la zona più colpita dal sisma, i cittadini cercano di rimuovere le macerie con ogni mezzo. Situazione critica in molti ospedali, in particolare tra Caracas e La Guaira: diverse strutture sono alle prese con carenze di acqua, antibiotici, soluzioni per flebo, anestetici.

–

internazionale/esteri

webinfo@adnkronos.com (Web Info)

Novità su Google, per aggiungere Key4Biz tra le tue fonti preferite, clicca qui

Leggi le altre notizie sull’home page di Key4biz

https://www.key4biz.it/terremoto-in-venezuela-ritrovato-vivo-un-bambino-di-11-anni/577774/

Estorsione senza cifratura: quando l’incidente cambia categoria giuridica (e le metriche smettono di dire la verità)

Per quindici anni il ransomware ha avuto una firma inconfondibile: i sistemi si bloccano, compare la richiesta di

riscatto, l’operatività si ferma. Quella firma era anche, di fatto, il suo *trigger* regolatorio: un impatto sulla disponibilità così evidente da non lasciare margini di interpretazione su cosa fosse accaduto e quando. Lo spostamento verso l’estorsione basata sul solo furto di dati, senza cifratura, viene di solito raccontato come una nuova tattica criminale. È una lettura riduttiva. La conseguenza più rilevante non è tattica ma di qualificazione: l’incidente migra dalla categoria della disponibilità a quella della riservatezza, e questo disallinea le metriche pubbliche, complica il momento da cui decorrono gli obblighi di notifica e attiva un doppio binario regolatorio che la maggior parte delle organizzazioni non ha ancora messo a terra.

I numeri, letti per quello che dicono davvero

Il primo equivoco da sciogliere riguarda la portata del fenomeno. L’esfiltrazione di dati non sostituisce la cifratura: l’accompagna, ormai quasi sempre. Secondo i dati trimestrali di Coveware (gruppo Veeam), nel secondo trimestre 2025 l’esfiltrazione ha avuto un ruolo in circa il 74 per cento dei casi gestiti, e il furto di dati ha superato la cifratura come leva estorsiva primaria. Altre rilevazioni collocano la quota di intrusioni con esfiltrazione vicino al 77 per cento, in netta crescita rispetto al 57 per cento del 2024.

Qui però va inserito il dato controintuitivo che rende il quadro più interessante, non meno. L’estorsione *encryptionless* presa come modello a sé, cioè il puro furto di dati senza alcuna cifratura, è un convertitore debole e strutturalmente basso. Secondo Coveware, nel terzo trimestre 2025 il tasso di pagamento per la sola esfiltrazione era sceso al 19 per cento, minimo assoluto per la categoria, per poi risalire intorno al 25 per cento nel quarto trimestre, restando comunque su

livelli storicamente contenuti. Il movimento di fondo è ancora più netto sui tassi di pagamento complessivi, che hanno rotto al ribasso la storica fascia 25-35 per cento, attestandosi al 23 per cento nel terzo trimestre e al 20 per cento nel quarto. La quinta campagna di esfiltrazione di massa del gruppo CL0P, costruita sullo sfruttamento di una vulnerabilità *zero-day* in Oracle E-Business Suite, ha reso bene questa perdita di efficacia: tanti dati sottratti, conversione economica deludente.

La sintesi corretta è quindi a due tempi. L'esfiltrazione come componente è diventata norma; l'estorsione senza cifratura come modello autonomo rende sempre meno. Eppure è proprio quest'ultima a creare i problemi più seri, e non sul piano economico.

Il paradosso statistico: la metrica cala mentre il rischio migra

Il report annuale di Kaspersky sullo stato del ransomware nel 2026 contiene un'apparente buona notizia: la quota di organizzazioni colpite da ransomware è scesa nel 2025 in tutte le regioni misurate dalla telemetria Kaspersky Security Network. Letta da sola, quella riga rassicura. Letta accanto ai dati sull'esfiltrazione, racconta l'opposto.

Il calo formale è in parte un artefatto di classificazione. Un attacco che non cifra nulla, ma sottrae dati e minaccia la pubblicazione, spesso non viene contato come "ransomware" nelle tassonomie costruite attorno all'evento di cifratura. La minaccia non diminuisce: cambia casella. E quella in cui si sposta è misurata con strumenti diversi (il monitoraggio dei *leak site*, le rivendicazioni sui portali criminali) o non misurata affatto, perché molte vittime di sola esfiltrazione preferiscono non emergere finché il dato non compare pubblicamente. Il risultato è che la metrica che decisori pubblici, stampa e board leggono per orientarsi, il numero di

“incidenti ransomware”, sottostima precisamente la direzione in cui il rischio si sta muovendo. Per chi fa misurazione a livello nazionale (ACN, Clusit) questo non è un dettaglio: è un problema di calibrazione strutturale degli indicatori.

Il caso italiano offre una conferma operativa di questa dinamica, ribaltata di segno. L’Operational Summary ACN di marzo 2026 registra 436 eventi cyber, sostanzialmente stabili rispetto ai 435 di febbraio, ma 313 incidenti a impatto confermato, in aumento dell’81 per cento sul mese precedente. La stessa Agenzia chiarisce che l’incremento non riflette un’esplosione degli attacchi, bensì la maggiore visibilità derivante dalla piena operatività degli obblighi di notifica NIS2, mentre gli impatti complessivi restano allineati alla media dei mesi precedenti. Tra le minacce prevalenti del mese figurano l’esposizione di dati e la violazione dei livelli di servizio attesi. È lo stesso paradosso, letto in positivo: il numero sale non perché il rischio cresca all’improvviso, ma perché finalmente lo si misura. E vale, a maggior ragione, il corollario inverso: fuori dal perimetro NIS2, e per le fattispecie che la cifratura non rende evidenti, una quota di rischio resta invisibile alle statistiche.

Da disponibilità a riservatezza: cosa cambia sotto NIS2

È sul piano normativo che lo spostamento diventa sostanza. La Direttiva NIS2, recepita in Italia con il decreto legislativo 4 settembre 2024, n. 138, definisce l’incidente significativo come l’evento, intenzionale o accidentale, che compromette in modo rilevante la disponibilità, l’integrità o la riservatezza dei sistemi informativi e di rete. La Determinazione ACN n. 379907/2025 traduce questa tripartizione in tipologie di incidente notificabili: gli allegati 3 e 4 individuano le fattispecie, distinguendo tre tipologie per i soggetti importanti (IS-1, perdita di riservatezza verso l’esterno di

dati digitali; IS-2, perdita di integrità con impatto verso l'esterno; IS-3, violazione dei livelli di servizio attesi) e una quarta, per i soli soggetti essenziali, riconducibile all'accesso non autorizzato o con abuso dei privilegi.

Il ransomware classico ricade dritto nella disponibilità, la fattispecie IS-3 della violazione dei livelli di servizio: impossibile non accorgersene, immediato classificarlo. L'estorsione senza cifratura cade invece nella IS-1, la perdita di riservatezza verso l'esterno. È comunque un incidente significativo, comunque notificabile. Ma si manifesta in modo silenzioso, si scopre tardi e, nei casi peggiori, si apprende dal *leak site* dell'attaccante o da una segnalazione di terzi prima che dai propri sistemi.

Il vero nodo operativo: quando scattano le 24 ore

Qui si apre la frattura che le procedure di *incident response* tarate sul vecchio modello non coprono. La determinazione ACN n. 379907/2025, efficace dal 15 gennaio 2026, conferma le tempistiche del decreto: pre-notifica al CSIRT Italia entro 24 ore, notifica completa entro 72 ore, relazione finale entro un mese. Il termine non decorre dal verificarsi dell'incidente, ma dall'acquisizione dell'evidenza, intesa come il momento in cui il soggetto dispone di elementi oggettivi che ne attestano l'avvenuto verificarsi.

Con un attacco a cifratura, quel momento è inequivocabile: i sistemi giù, la nota di riscatto. Con l'esfiltrazione silenziosa, l'evidenza è un concetto scivoloso. Scatta quando l'analisi rileva indicatori di compromissione settimane dopo l'accesso iniziale? Quando un fornitore segnala un'anomalia? Quando il dato compare sul portale criminale? Le Linee Guida ACN ammettono esplicitamente che l'evidenza possa emergere anche molto dopo l'inizio dell'incidente, e indicano tra le fonti di acquisizione anche le segnalazioni esterne, comprese

quelle del CSIRT stesso. Tradotto in termini operativi: un'organizzazione può trovarsi con il cronometro delle 24 ore avviato da una notizia che arriva dall'esterno, su un evento di cui non aveva contezza, mentre il modello di estorsione senza cifratura è progettato apposta per restare sotto i radar il più a lungo possibile. La detection arretrata, in questo scenario, non è solo un fallimento di sicurezza: è un fallimento di conformità.

C'è poi un dettaglio nella struttura della determinazione che chiude il paradosso su se stesso. La soglia di significatività non è lasciata alla discrezione del soggetto: il testo aggancia le fattispecie a una misura tecnica precisa, la DE.CM-01, che fissa i livelli di servizio atteso (SL) e i parametri quali-quantitativi di riferimento. Ma l'aggancio non è simmetrico, ed è qui che la categoria dell'incidente fa la differenza. La violazione dei livelli di servizio (IS-3), in cui ricade il ransomware a cifratura, è notificabile al superamento delle soglie SL stabilite ai sensi della DE.CM-01: esiste cioè un cancello quantitativo che media tra l'evento e l'obbligo. La perdita di riservatezza verso l'esterno (IS-1), la casella dell'estorsione senza cifratura, nel testo dell'allegato non porta con sé alcun parametro quantitativo: è la semplice evidenza della fuga di dati a renderla notificabile. Ne segue una conclusione controintuitiva ma rigorosa: l'attacco più silenzioso, quello che si fatica a rilevare, è anche quello con la soglia di notifica più bassa e meno graduabile. Una volta acquisita l'evidenza, il cronometro parte senza la mediazione di un livello-soglia da superare.

Il doppio binario ACN e Garante

C'è un secondo livello di complessità. Quando l'incidente di riservatezza coinvolge dati personali, e nell'estorsione per furto dati è quasi sempre così, si attivano in parallelo due regimi distinti con due autorità, due cronometri e due valutazioni del rischio. Il GDPR impone la notifica della

violazione dei dati personali al Garante entro 72 ore ai sensi dell'articolo 33; la NIS2 impone la pre-notifica al CSIRT Italia entro 24 ore. Le due scadenze non coincidono, e neppure i criteri di valutazione: la NIS2 ragiona sulla compromissione di reti e sistemi nel loro complesso, il GDPR sulla protezione degli interessati.

La cooperazione tra ACN e Garante è prevista ex lege dall'articolo 14 del decreto, che al comma 2 contempla la comunicazione, da parte dell'Agenzia e senza indebito ritardo, di ogni violazione degli obblighi di notifica suscettibile di configurare anche una violazione di dati personali. Ma non esiste ancora un portale unico nazionale: l'onere del coordinamento resta sull'organizzazione, che deve far convivere due procedure con tempistiche diverse senza trasmettere alle due autorità versioni discordanti dello stesso evento. Per il settore finanziario il quadro si complica ulteriormente, perché DORA opera come *lex specialis* e prevale con un proprio impianto di segnalazione. L'estorsione senza cifratura, in sostanza, è proprio la tipologia di incidente che massimizza la sovrapposizione tra i regimi, perché tocca insieme la riservatezza dei sistemi e i dati personali, mentre il ransomware a sola cifratura, se non esfiltra, può in alcuni casi restare confinato al perimetro NIS2.

Il caso Eataly del giugno 2026 mostra il doppio binario in azione. A fronte di un attacco all'infrastruttura che ospita l'e-commerce, l'azienda ha notificato l'incidente alle autorità competenti ai sensi sia della NIS2 sia del GDPR, e la comunicazione via email ai clienti è valsa come notifica agli interessati ex articolo 34 del GDPR. È un incidente che non ruota attorno alla cifratura ma attorno all'accesso e alla potenziale esposizione di dati anagrafici, codici fiscali e storico acquisti; nelle prime analisi l'azienda ha anzi dichiarato di non aver riscontrato un download dei dati, e il doppio regime di notifica è scattato comunque. È la

dimostrazione concreta che, una volta spostato il baricentro sulla riservatezza, il *trigger* non richiede né il blocco dei sistemi né la prova di un'esfiltrazione completata: basta il rischio per i diritti degli interessati e la riconducibilità a una fattispecie significativa.

La trappola di compliance e l'incentivo al silenzio

L'assenza di blocco operativo genera un incentivo perverso. Quando i sistemi continuano a funzionare, la tentazione di gestire l'evento in silenzio, magari pagando, è strutturalmente più alta che davanti a una linea di produzione ferma. È esattamente la condizione in cui la mancata notifica diventa una seconda violazione che si somma alla prima. La violazione degli obblighi di notifica dell'articolo 25 ricade nel regime sanzionatorio dell'articolo 38 del D.Lgs. 138/2024, che prevede, per i soggetti essenziali, sanzioni fino a 10 milioni di euro o al 2 per cento del fatturato mondiale annuo, e per i soggetti importanti fino a 7 milioni o all'1,4 per cento. E poiché il modello *encryptionless* monetizza attraverso la pubblicazione sul *leak site*, la scommessa del silenzio è anche fragile: il dato emerge comunque, spesso dopo che le finestre di notifica si sono chiuse.

Cosa cambia, concretamente, per il CISO

La conseguenza pratica è che il *playbook* di risposta non può più essere costruito attorno al ripristino. Le tre direttrici da rivedere sono nitide. La prima è la detection: il presidio va spostato dalla rilevazione della cifratura, evento tardivo e rumoroso, alla rilevazione dell'esfiltrazione, evento precoce e silenzioso, con strumenti di *data loss prevention*, monitoraggio dei flussi in uscita e analisi degli accessi a

identità e *workflow* privilegiati, che restano oggi il vettore iniziale dominante. La seconda è la prontezza alla notifica: la procedura deve registrare con precisione il *timestamp* dell'evidenza e gestire il doppio binario ACN-Garante con tempistiche pre-coordinate, non improvvisate nelle 24 ore. La terza è il disallineamento delle tassonomie, che vale anche per le polizze: una copertura cyber con clausole costruite sul concetto di ransomware-come-cifratura può non rispondere a un'estorsione di sola esfiltrazione, e questo va verificato prima dell'incidente, non durante.

Il punto di fondo è che l'apparato di misurazione e quello regolatorio sono ancora tarati su un modello centrato sulla disponibilità, mentre la superficie di rischio e l'esposizione giuridica si sono spostate sulla riservatezza. Finché questo scarto resta, il numero che rassicura nei report sarà lo stesso che nasconde dove il rischio è andato a posarsi. Per chi deve decidere budget e priorità, leggere quel numero per quello che non dice è già una forma di difesa.

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/articoli/estorsione-senza-cifratura/