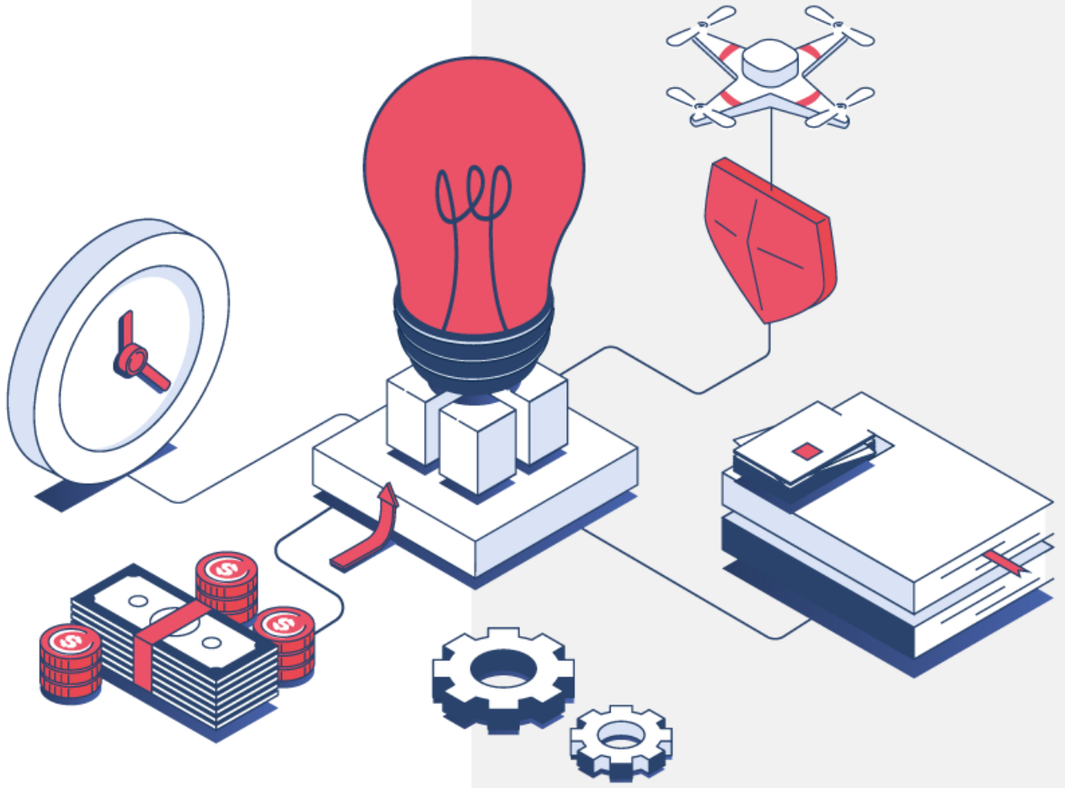
S3K

Cyber Threat

WEEKLY REPORT

\ week 13/04/2026 - 19/04/2026



www.s3kgroup.it

Aumento delle vulnerabilità critiche

Identificata una vulnerabilità critica in Protobuf e rilasciati exploit proof-of-concept per diverse vulnerabilità zero-day, richiedendo aggiornamenti urgenti da parte delle organizzazioni italiane.

Campagne di attacco mirate

Emersa una nuova campagna del GRU russo contro aziende occidentali, con implicazioni dirette per le organizzazioni italiane nei settori logistico e tecnologico.

Violazioni di dati significative

Diverse aziende, tra cui McGraw Hill e Basic-Fit, hanno subito violazioni di dati, esponendo milioni di account e aumentando il rischio di phishing per gli utenti italiani.

Attività ransomware in crescita

Il gruppo AKIRA ha intensificato gli attacchi ransomware in Italia, colpendo principalmente piccole e medie imprese e sfruttando vulnerabilità note nei firewall.

Evoluzione delle tecniche di phishing

Registrate campagne di phishing avanzate in Italia, tra cui smishing che sfrutta il nome di INPS, evidenziando la necessità di una maggiore consapevolezza tra gli utenti.

Necessità di aggiornamenti tempestivi

Il Patch Tuesday di Microsoft ha rilasciato 165 aggiornamenti: le organizzazioni devono mantenere i propri sistemi aggiornati per mitigare i rischi associati a vulnerabilità critiche attivamente sfruttate.

Notizie cyber della Settimana

Negli ultimi sette giorni, il panorama della sicurezza informatica ha visto un aumento significativo delle vulnerabilità e degli attacchi, con notizie che spaziano da exploit critici a campagne di cyber attacco mirate. Le organizzazioni, in particolare quelle italiane ed europee, devono prestare attenzione a queste minacce emergenti, che evidenziano la necessità di rafforzare le misure di sicurezza e la resilienza informatica.

- **Vulnerabilità critica in Protobuf:** Pubblicato un exploit proof-of-concept per una vulnerabilità di esecuzione di codice remoto nella libreria protobuf.js, ampiamente utilizzata in JavaScript. Impatti significativi su molte applicazioni web. Bleepingcomputer
- **Aumento degli attacchi nel Regno Unito:** Il NCSC ha segnalato un record di attacchi informatici, con quattro attacchi significativi a settimana, evidenziando rischi per le infrastrutture critiche. Cyble
- **Zero-day in Microsoft Defender:** Un ricercatore ha rilasciato un exploit proof-of-concept per una vulnerabilità zero-day in Microsoft Defender, sollevando preoccupazioni sulla collaborazione con i ricercatori di sicurezza. Bleepingcomputer
- **Vulnerabilità nei servizi Webex di Cisco:** Cisco ha rilasciato aggiornamenti di sicurezza per quattro vulnerabilità critiche nei suoi servizi Webex, richiedendo azioni da parte dei clienti. Bleepingcomputer
- **Campagna di attacchi russi contro aziende occidentali:** Un nuovo avviso ha rivelato una campagna del GRU russo mirata ad aziende logistiche e tecnologiche occidentali, con implicazioni dirette per le organizzazioni europee. Thecyberexpress
- **Breach di Vercel:** La piattaforma cloud Vercel ha confermato una violazione dei dati, con attori minacciosi che affermano di vendere dati rubati. Bleepingcomputer
- **Sanzione privacy ad ITA:** Il Garante della privacy ha multato la compagnia aerea ITA per violazioni del GDPR, evidenziando l'importanza della conformità alle normative. Cybersecurity360
- **Attività ostili su servizi VNC:** Lo CSIRT Italia ha segnalato un incremento delle attività ostili su servizi di accesso remoto VNC, spesso esposti in modo inadeguato. CSIRT IT

La settimana ha evidenziato un panorama di minacce in continua evoluzione, con vulnerabilità critiche e attacchi mirati che richiedono un'attenzione costante. È fondamentale che le aziende adottino misure proattive per proteggere i propri sistemi e dati.

GRU russo nel mirino: campagna contro aziende logistiche e tecnologiche occidentali

Un nuovo avviso di cybersecurity ha rivelato una campagna attribuita al GRU russo, mirata ad aziende logistiche e tecnologiche occidentali. Questo vettore di attacco rappresenta una minaccia concreta per le organizzazioni italiane che operano in questi settori, con possibili ripercussioni su supply chain e infrastrutture digitali.

Campagna GRU contro aziende occidentali

Il GRU russo ha condotto operazioni mirate contro aziende logistiche e tecnologiche, con obiettivi di spionaggio industriale e sabotaggio delle supply chain europee.

Zero-day Microsoft Defender

Un exploit proof-of-concept per una vulnerabilità zero-day in Microsoft Defender è stato reso pubblico, richiedendo aggiornamenti immediati da parte delle organizzazioni che utilizzano questo prodotto.

Vulnerabilità Webex di Cisco

Quattro vulnerabilità critiche nei servizi Webex di Cisco richiedono interventi urgenti da parte dei clienti per mitigare rischi di compromissione delle comunicazioni aziendali.

Rischio per l'Italia

Le organizzazioni italiane nei settori logistico e tecnologico sono esposte a rischi diretti. Il breach di Vercel e la sanzione a ITA evidenziano ulteriori vettori di vulnerabilità.

Obiettivi e superfici di attacco

- Aziende logistiche con infrastrutture IT esposte
- Piattaforme tecnologiche e cloud provider
- Servizi di collaborazione (Webex, VNC)
- Librerie JavaScript ampiamente utilizzate (protobuf.js)
- Sistemi Microsoft Defender non aggiornati
- Infrastrutture con scarsa igiene informatica

Aggiornare immediatamente i sistemi che utilizzano protobuf.js e Microsoft Defender. Verificare le configurazioni dei servizi Webex e limitare l'esposizione dei servizi VNC. Monitorare le attività sospette nelle reti aziendali.

Data Leak & Breach: Scenario Settimanale

Negli ultimi sette giorni, il panorama delle violazioni di dati ha visto un incremento significativo di incidenti, coinvolgendo aziende di vari settori, tra cui l'istruzione e il fitness. Diverse organizzazioni hanno subito attacchi mirati, con dati sensibili esposti e minacce di estorsione da parte di gruppi di cybercriminali.

13.5M

Account McGraw Hill

Violazione causata da una configurazione errata di Salesforce, con esposizione di email, nomi e dati di contatto.

1M

Membri Basic-Fit colpiti

Una delle più grandi catene di fitness in Europa ha subito una violazione che ha esposto i dati di un milione di membri.

45M

Record Salesforce minacciati

La gang ShinyHunters ha minacciato di divulgare 45 milioni di record se non fosse stato pagato un riscatto.

1.6M

Credenziali italiane in vendita

Una combinazione di 1,6 milioni di credenziali italiane è stata messa in vendita su forum del dark web.

Ulteriori violazioni hanno coinvolto **Rockstar Games** (dati analitici rubati dalla gang ShinyHunters tramite un incidente presso Anodot), **Booking.com** (accesso non autorizzato con esposizione di dati di prenotazioni e utenti) e il **Silent Ransom Group** (evoluzione nelle strategie di attacco mirate a studi legali). La settimana ha evidenziato l'importanza di rafforzare le misure di protezione dei dati a tutti i livelli.

RISCHI SETTIMANALI

Top 5 Rischi Cyber per l'Italia

Rischio	Impatto/Dettaglio	Azione Raccomandata
🔴 Campagna GRU su Supply Chain	Impatto: Alto | Target: Logistica, Tecnologia	Monitorare anomalie su accessi e traffico di rete
🔴 Ransomware AKIRA su PMI Italiane	Impatto: Alto | Vettore: Firewall SonicWall / VPN vulnerabili	Patch + hardening accessi remoti
🟠 Phishing Avanzato (INPS, Apple, AI Vishing)	Impatto: Alto | Trend: Smishing + voice phishing automatizzato	Awareness utenti + MFA
🟠 Exploit Pubblici (Protobuf, Defender, Axios)	Impatto: Alto | Rischio: RCE e compromissioni rapide	Patch immediate e verifica librerie
🟡 Data Leak e Credenziali Italiane (1.6M)	Impatto: Medio-Alto | Rischio: Credential stuffing e phishing mirato	Reset password + monitoraggio dark web

Minacce per Settori Critici: Dettaglio Breach

Istruzione & Editoria

McGraw Hill ha confermato una violazione che ha compromesso 13,5 milioni di account a causa di una configurazione errata di Salesforce. I dati esposti includono indirizzi email, nomi e informazioni di contatto, aumentando il rischio di phishing.

Settore Fitness & Sport

Basic-Fit, una delle più grandi catene di fitness in Europa, ha subito una violazione che ha esposto i dati di un milione di membri, sottolineando l'importanza della sicurezza nei sistemi di gestione dei dati dei clienti.

Turismo & Hospitality

Booking.com ha rivelato un accesso non autorizzato ai suoi sistemi, che ha esposto dati sensibili relativi a prenotazioni e utenti. Gli utenti sono stati avvisati di modificare i loro PIN per proteggere le loro informazioni.

Tecnologia & Gaming

I dati analitici di Rockstar Games sono stati rubati e divulgati dalla gang ShinyHunters. Tre vulnerabilità recentemente divulgate di Windows sono state sfruttate in attacchi mirati per ottenere permessi elevati nelle organizzazioni europee.

Malware & Infrastructure

Negli ultimi sette giorni, il panorama delle minacce informatiche ha mostrato un'attività intensa nel settore del malware e delle infrastrutture. Diverse campagne malevole hanno preso di mira sistemi industriali, sanitari e piattaforme di gestione dei contenuti come WordPress. Le nuove famiglie di malware, come ZionSiphon e AgingFly, evidenziano l'evoluzione delle tecniche di attacco.

Principali Incidenti e Minacce

1. **ZionSiphon – Infrastrutture idriche:** Nuovo malware progettato per compromettere i sistemi di trattamento dell'acqua, evidenziando il rischio per le infrastrutture critiche con potenziali ripercussioni sulla sicurezza delle risorse idriche.
2. **AgingFly – Spionaggio sanitario:** Malware utilizzato in attacchi mirati a ospedali e enti governativi in Ucraina, rubando dati di autenticazione da browser e applicazioni di messaggistica.
3. **Compromissione plugin WordPress:** Oltre 30 plugin della suite EssentialPlugin sono stati compromessi, permettendo accessi non autorizzati a migliaia di siti web.
4. **Falso SDK Zoom su macOS:** Un attacco ha sfruttato un falso aggiornamento dell'SDK di Zoom per diffondere malware Sapphire Sleet su macOS, evidenziando l'evoluzione delle tecniche di ingegneria sociale.

Nuovi Malware Identificati

PowMix – Botnet Repubblica Ceca

Botnet attiva dal dicembre 2025 scoperta da Cisco Talos, che colpisce un'ampia fascia di lavoratori in Repubblica Ceca. Nuova minaccia per le organizzazioni locali.

MiningDropper – Android

Crescita significativa delle campagne che utilizzano MiningDropper, un framework di malware modulare per Android con impatto su un gran numero di utenti mobili.

Storm – Infostealer

Malware che utilizza tecniche avanzate per eludere la decrittazione locale, inviando dati del browser direttamente ai server degli attaccanti. Nuova frontiera nel furto di dati.

Malfixer – Anti-Analisi APK

Nuova tecnica di malformazione degli APK come metodo anti-analisi, con tool Malfixer progettata per rilevare e riparare APK malformati e migliorare le capacità di risposta.

Le organizzazioni italiane ed europee devono adottare misure proattive contro malware specializzati e aggiornare i sistemi di rilevamento per identificare nuove varianti come ZionSiphon, AgingFly e Storm in circolazione.

Phishing & Social Engineering

Negli ultimi sette giorni, il panorama del phishing e del social engineering ha mostrato un'attività intensa, con diverse campagne malevole che hanno preso di mira utenti e organizzazioni, in particolare in Italia. Le tecniche di attacco si sono evolute, sfruttando notifiche legittime e piattaforme automatizzate per ingannare le vittime, con un uso crescente dell'intelligenza artificiale.

01

Abuso notifiche Apple

Le notifiche di cambio account Apple sono state sfruttate per inviare email di phishing riguardanti acquisti di iPhone, aumentando la legittimità apparente e la capacità di eludere i filtri antispam.

02

Piattaforma di vishing ATHR

Lanciata una piattaforma di voice phishing automatizzata che utilizza agenti vocali AI per raccogliere credenziali, combinando operatori umani e tecnologia per una fase di social engineering più efficace.

03

Campagne CERT-AGID in Italia

Il CERT-AGID ha registrato 128 campagne malevole, di cui 96 mirate a obiettivi italiani. Tra queste, una campagna di smishing che utilizza il nome di INPS per raccogliere dati personali e lavorativi.

04

Smishing INPS

Nuova campagna di smishing che richiede informazioni sensibili come cedolini e documenti identificativi, con tecniche di urgenza per indurre le vittime a fornire i dati richiesti.

05

BlobPhish – Phishing invisibile

Identificata una nuova tecnica di phishing che nasconde le pagine malevole nella memoria del browser, rendendo difficile la loro rilevazione da parte dei sistemi di sicurezza.

06

Protezione Microsoft file RDP

Microsoft ha introdotto nuove protezioni contro attacchi di phishing che sfruttano file di connessione Remote Desktop, disabilitando risorse condivise rischiose per impostazione predefinita.

07

Operazione FBI contro W3LL

Le autorità statunitensi e indonesiane hanno smantellato una rete di phishing globale, arrestando il presunto sviluppatore del kit W3LL, che aveva colpito oltre 17.000 vittime.

Tecniche Avanzate Emergenti

- Voice phishing automatizzato con AI (piattaforma ATHR)
- BlobPhish: phishing nascosto nella memoria del browser
- Abuso di notifiche di servizi legittimi (Apple)
- Smishing con impersonificazione di enti governativi (INPS)

Target Principali Italiani

- Utenti INPS (smishing per dati lavorativi)
- Utenti Apple (notifiche di acquisto fraudolente)
- Pubblica Amministrazione (128 campagne CERT-AGID)
- Clienti Booking.com (attacco post-breach)

Operazioni Ransomware Attive

Negli ultimi sette giorni, il panorama degli attacchi ransomware ha mostrato un'attività intensa, con diversi gruppi di cybercriminali che hanno rivendicato attacchi contro aziende italiane e internazionali. È stato segnalato un aumento significativo degli attacchi in Italia, con particolare attenzione al gruppo AKIRA, che sfrutta vulnerabilità nei sistemi di sicurezza.

Incremento AKIRA in Italia

Il CSIRT Italia ha segnalato un aumento significativo di attacchi ransomware attribuiti al gruppo AKIRA, con 13 incidenti confermati principalmente contro piccole e medie imprese. Le vulnerabilità sfruttate riguardano firewall SonicWall e servizi SSL VPN.

Lockbit5 colpisce aziende italiane

Il gruppo Lockbit5 ha pubblicato nuovi bersagli italiani, tra cui contrar.it, seleniaravenna.it e wibeats.it, evidenziando la loro continua attività nel panorama ransomware nazionale.

Attacco a Servetto-Srl

Il gruppo "lamashtu" ha rivendicato un attacco contro Servetto-Srl, con il sito servetto.it compromesso.
Hash: cec4b3c2d1123efbd13610da31c2e0778bb5a0afdcd7d38aa565511019ba219d.

Attacco a IC-Partners

Il gruppo ransomware "thegentlemen" ha rivendicato un attacco contro IC-Partners, con il sito web icpartners.it compromesso. Hash: 53aceff3f705a4abfc48ca04119ee50f7be7f2260c9a48134ab4c4184d8d3563.

Attacco a ASTM-Group

Il gruppo "coinbasecartel" ha attaccato ASTM-Group, compromettendo il sito astim.it. Hash: b7a746ab3ad7dbdcf0617c21afba0e8e0105e99617076e32d8a2e2489bb80b33.

ShinyHunters & Ransomware Payouts King

Il gruppo ShinyHunters ha rivendicato attacchi contro diverse aziende tra cui Zara e Carnival Corporation. Il ransomware Payouts King utilizza QEMU VMs per bypassare la sicurezza degli endpoint eseguendo macchine virtuali nascoste.

Vulnerabilità Critiche & Patch

Negli ultimi sette giorni, il panorama delle vulnerabilità ha visto un'attività intensa, con Microsoft che ha rilasciato il Patch Tuesday di aprile risolvendo 165 vulnerabilità, tra cui due di tipo zero-day. Diverse vulnerabilità critiche sono state scoperte e sfruttate attivamente. Le organizzazioni italiane ed europee sono esortate a mantenere i propri sistemi aggiornati.

1	**Patch Tuesday Microsoft – 165 aggiornamenti** Rilasciati 165 aggiornamenti di sicurezza, inclusi due zero-day. Le vulnerabilità riguardano Denial of Service e Remote Code Execution. Aggiornare i sistemi per prevenire exploit attivi. CSIRT Italia
2	**CVE-2026-32196 – Windows Admin Center** Disponibile un Proof of Concept (PoC) per questa vulnerabilità critica. Si raccomanda un aggiornamento immediato del software per evitare sfruttamenti. CSIRT Italia
3	**CVE-2026-33032 – Nginx UI** Vulnerabilità critica che consente il takeover completo del server Nginx. È attivamente sfruttata in rete, rendendo urgente l'implementazione di patch. Over Security
4	**CVE-2026-34197 – Apache ActiveMQ** Rilevato sfruttamento attivo di questa vulnerabilità. Si consiglia di aggiornare il software per mitigare i rischi. CSIRT Italia
5	**CVE-2026-40175 – Axios** Disponibile un PoC per questa vulnerabilità che consente Authentication Bypass e Remote Code Execution. Cruciale mantenere aggiornati i sistemi che utilizzano questa libreria. CSIRT Italia
6	**CVE-2026-5173 – GitLab** Un PoC per questa vulnerabilità è stato reso pubblico, evidenziando la necessità di aggiornamenti tempestivi per evitare Denial of Service e bypass delle restrizioni di sicurezza. CSIRT Italia
7	**CVE-2026-6264 – Talend** Vulnerabilità critica che consente l'esecuzione remota di codice senza autenticazione. Le versioni vulnerabili devono essere aggiornate urgentemente. CVE Monitor
8	**CVE-2026-4682 – HP DeskJet** Alcuni modelli di stampanti HP sono vulnerabili a potenziali exploit di codice remoto. È consigliato aggiornare il firmware per mitigare i rischi. CVE Monitor

Analisi Trasversale e Tendenze

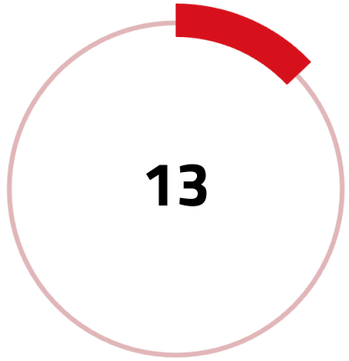
Negli ultimi sette giorni, il panorama della cybersecurity ha evidenziato un incremento preoccupante delle vulnerabilità e degli attacchi, con un focus particolare su exploit critici e campagne di cyber attacco mirate. Le organizzazioni italiane ed europee si trovano ad affrontare una crescente varietà di minacce, che spaziano da vulnerabilità nei software più utilizzati a campagne di phishing sofisticate e attacchi ransomware sempre più mirati.

Rispetto alle settimane precedenti, si osserva un aumento significativo degli attacchi ransomware, con gruppi noti come AKIRA e Lockbit5 che continuano a colpire le piccole e medie imprese italiane. L'emergere di malware specializzati come ZionSiphon per le infrastrutture idriche e l'uso di tecniche avanzate di social engineering come il vishing automatizzato pongono nuove sfide per la sicurezza informatica. Il rilascio di 165 patch Microsoft sottolinea l'urgenza di un approccio proattivo alla gestione delle vulnerabilità.

Tendenze chiave: campagne GRU russo contro aziende occidentali, attacchi AKIRA alle PMI italiane tramite firewall SonicWall, smishing INPS e phishing multicanale, e violazioni di dati massicce nel settore education e fitness.

Patch Microsoft Aprile

Aggiornamenti di sicurezza rilasciati nel Patch Tuesday, inclusi due zero-day attivamente sfruttati (12/04/2026 – 19/04/2026)



Attacchi AKIRA Confermati

Incidenti ransomware confermati dal CSIRT Italia, principalmente contro PMI con firewall SonicWall vulnerabili

Campagne Malevole CERT-AGID

Campagne malevole registrate nella settimana, di cui 96 specificamente mirate a obiettivi italiani

Tendenze Emergenti

- Campagne GRU russo contro settori logistici e tecnologici
- Ransomware AKIRA su PMI italiane (firewall SonicWall)
- Smishing con impersonificazione INPS
- Vishing automatizzato con AI (piattaforma ATHR)

Settori più Colpiti

- Piccole e medie imprese italiane (AKIRA, Lockbit5)
- Istruzione ed editoria (McGraw Hill)
- Fitness e turismo (Basic-Fit, Booking.com)
- Infrastrutture critiche (idriche, ospedali ucraini)

Raccomandazioni Operative Prioritarie

Per affrontare le sfide della settimana, è fondamentale che le organizzazioni adottino un approccio proattivo alla sicurezza informatica. Il contesto in continua evoluzione delle minacce richiede particolare attenzione su più fronti, con priorità agli aggiornamenti critici e alla formazione del personale.

Priorità immediate:

- Applicare immediatamente le 165 patch del Patch Tuesday Microsoft, con priorità assoluta per le due vulnerabilità zero-day attivamente sfruttate.
- Aggiornare i sistemi che utilizzano Nginx UI (CVE-2026-33032), Apache ActiveMQ (CVE-2026-34197), Axios (CVE-2026-40175) e GitLab (CVE-2026-5173).
- Verificare e aggiornare le configurazioni dei firewall SonicWall e dei servizi SSL VPN per prevenire gli attacchi del gruppo AKIRA.
- Aggiornare il firmware delle stampanti HP DeskJet vulnerabili (CVE-2026-4682) e i sistemi Talend (CVE-2026-6264).

Misure di sicurezza strutturali:

- Investire in programmi di formazione per sensibilizzare i dipendenti sui rischi del phishing, con focus su smishing INPS, abuso notifiche Apple e vishing automatizzato con AI.
- Implementare l'autenticazione a più fattori per proteggere le credenziali aziendali, in particolare per i servizi cloud e le piattaforme di collaborazione come Webex.
- Monitorare attivamente il dark web per rilevare la vendita di credenziali italiane (1,6 milioni di credenziali compromesse) e dati aziendali sensibili.
- Implementare strategie di backup e ripristino dei dati per garantire la resilienza in caso di attacchi ransomware, con particolare attenzione alle PMI italiane bersagliate da AKIRA.
- Limitare l'esposizione dei servizi VNC e verificare le configurazioni dei sistemi di accesso remoto segnalati dallo CSIRT Italia come vettori di attacco attivi.

COMPANY PROFILE S3K

Tutto il nostro essere è racchiuso nella nostra VISION: “Rendere il mondo digitale un luogo accessibile, sicuro e sostenibile, al servizio della conoscenza”

COME LO FACCIAMO

Ci posizioniamo in modo unico nel mercato in cui operiamo, sia grazie ad una precisa offerta multidisciplinare integrata, che al nostro approccio volutamente orientato alla semplificazione di tutto ciò che riguarda i processi di Digital e Security Transformation.
Abbiamo un presidio esteso sul territorio con circa 550 dipendenti distribuiti tra le sedi di Roma, Milano, Torino, Padova, Firenze, Palermo e Catania. L’ambizione e la prospettiva vedono un ulteriore e progressivo rafforzamento sia sul territorio nazionale che internazionale dove già operiamo con successo e con Clienti di primaria rilevanza.

CON QUALI LEVE OPERIAMO

Le nostre competenze principali: Data Analytics & Big Data, CyberSecurity, Application Development, Infrastructure Management, Cloud & Managed Security Services.
Più caratteristiche sono poi le nostre competenze verticali, nel novero delle quali particolare attenzione va al PLM, Modelling & Simulation (la società di S3K, Fabaris, è l'unica azienda italiana che sa utilizzare il sistema di modellazione e simulazione jtls (joint theatre level simulation) utilizzato dalla Nato)) e Digital Transaction Management, Business Operation Systems.
40 partnership strategiche, 215 certificazioni professionali, un’esperienza complessiva che sfiora i 150 anni uomo, ed oltre 500 clienti attivi.

CHI SIAMO

Un FULL SERVICE PARTNER DELLA DIGITAL & SECURITY TRANSFORMATION. Ci posizioniamo in modo unico nel mercato in cui operiamo, sia grazie ad una precisa offerta multidisciplinare integrata, che al nostro approccio volutamente orientato alla semplificazione di tutto ciò che riguarda i processi di Digital e Security Transformation.
S3K nasce nel dicembre 2021 come fusione di importanti realtà già operanti su questi mercati in seguito all’ingresso di un importante Private Equity internazionale (HLD).

CONTATTI:
contattaci@s3kgroup.it
insidesales@s3kgroup.it
marketing@s3kgroup.it

Cyber security

RISK REPORT

S3K

Via del Serafico, 200 - 00142 | Roma (RM)
C.S.iv. € 10.050.000,00 - C.F. e P.IVA: 15379561002

ISO 14001 BUREAU VERITAS Certification

ISO 27001 BUREAU VERITAS Certification

ISO 9001 BUREAU VERITAS Certification

ISO 45001 BUREAU VERITAS Certification