USA denunciano furto di migliaia di email. Dito puntato sulla Russia



Continuano le denunce da parte di Washington di presunte campagne informatiche a suo danno sponsorizzate da Paesi stranieri. Questa è l'accusa che da più parti, nell'intelligence americana, viene rivolta senza troppi mezzi termini verso la Cina, ma molto più spesso verso la Russia.

Il furto e i sospetti sulla Russia

Secondo quanto riportato da *politico.com*, due fonti interne al Congresso hanno reso noto che nel 2020 sono state **rubate migliaia di email di funzionari del Dipartimento di Stato** e che dietro a questa cyber operazione c'è uno Stato sponsor molto potente, molto probabilmente la Russia.

In particolare, avrebbero rivelato le fonti interne a Washington, gli uffici del Dipartimento che avrebbero subito le maggiori violazioni sarebbero l'Ufficio per gli affari europei ed euroasiatici e l'Ufficio per gli affari in Asia orientale e del Pacifico.

Salva, a quanto pare, la rete interna che porta ai documenti più sensibili e le informazioni classificate.

Non è ancora chiaro, però, se tale denuncia rientra nei cyber attacchi a cui è stata sottoposta **SolarWinds**, o se faccia parte di una campagna di cyber spionaggio del tutto nuova.

Blindare la sicurezza interna

Secondo quanto fatto trapelare dal Dipartimento stesso, "*prendiamo molto seriamente la nostra responsabilità in termini di protezione e salvaguardia delle informazioni in nostro possesso e adottiamo continuamente nuove misure sempre più sofisticate ed efficaci di cybersecurity per garantire questo livello di protezione*".

"*Per motivi di sicurezza nazionale non siamo autorizzati a discutere circa la natura di eventuali e presunti incidenti di sicurezza informatica*", è specificato nella comunicazione, si legge sempre su Politico.

Il vice consigliere per la Sicurezza nazionale e per le nuove tecnologie, **Anne Neuberger**, ha inoltre dichiarato che "*diverse Agenzie federali americane sono state oggetto di attacchi informatici nell'ultimo anno e alcune di esse sono state violate*".

"*Nell'ambito dei fatti relativi a SolarWinds* – ha affermato Neuberger – *abbiamo scoperto grandi vulnerabilità nelle difese informatiche dell'amministrazione e delle agenzie federali. Abbiamo identificato cinque aree specifiche su cui insistere per modernizzare la cybersecurity e stiamo implementando un*

piano di investimenti dedicato a tali tecnologie per potenziare definitivamente il nostro apparato di sicurezza informatica".

Nonostante gli attacchi e le discussioni mediatiche attorno al tema della sicurezza nazionale, **la Casa Bianca deve ancora nominare un direttore per la sicurezza informatica del Paese**, con il compito non semplice di coordinare l'azione di Governo in termini di cybersecurity e di contrasto ai piani di cyber spionaggio internazionali.

Biden VS Putin

Da quando **Joe Biden** è Presidente degli Stati Uniti non sono mai mancati gli attacchi alla Russia, soprattutto per le interferenze nella vita politica interna americana, nelle elezioni americane, nella disinformazione via social, nel tentativo di creare una divisione insanabile all'interno della più grande democrazia del mondo.

Non ultimo quello più recente in cui si accusa direttamente **Vladimir Putin** di essere "un assassino", "un killer", soprattutto in riferimento all'avvelenamento di **Alexey Navalny** e a tanti altri fatti simili mai chiariti negli anni.

https://www.key4biz.it/usa-denunciano-furto-di-migliaia-di-email-dito-puntato-sulla-russia/353361/

Australia, attacco informatico al Parlamento.

Sospettata la Cina



In Australia il Parlamento sta indagando su una grave interruzione tecnica che, durante il fine settimana, ha bloccato l'accesso della posta elettronica a deputati e senatori, sollevando la preoccupazione di un esteso cyber-attacco.

Attacco hacker all'Australia: cosa sta succedendo

Secondo quanto riportano i media australiani l'interruzione principale è iniziata intorno a mezzogiorno di sabato con un accesso limitato e in alcuni casi senza accesso a dispositivi IT o mobili per oltre 30 ore da parte dei parlamentari.

Un portavoce del Dipartimento dei servizi parlamentari (DPS) – che sovrintende al Parlamento a Canberra – ha affermato che

alcuni servizi su smartphone e tablet emessi dal DPS sono stati interrotti e non tutti sono tornati alla normalità.

"Il Department Parlamentary Services sta anche lavorando per indagare sulla causa dell'interruzione e l'Australian Cyber Security Center sta fornendo consulenza come parte di tale processo", ha detto il portavoce. *"DPS sta lavorando per risolvere i problemi e alcuni servizi sono stati ripristinati."*

Il viceministro della Difesa **Andrew Hastie** ha rivelato a News.com.au che il governo **Morrison** è stato costretto a tagliare l'accesso all'IT e alle e-mail del Parlamento per proteggersi da un attacco informatico relativo ad un attaccante esterno.

"La causa dell'interruzione ai servizi IT è dovuta ad un agente esterno e, una volta rilevato il problema, la connessione ai sistemi governativi è stata interrotta immediatamente per precauzione", ha dichiarato Hastie. *"L'Australian Cyber Security Center è stato in contatto con il DPS fornendo supporto e continuando a monitorare la situazione. La sicurezza informatica è un lavoro di squadra e una responsabilità condivisa. È fondamentale che le aziende e le organizzazioni australiane siano attente a questa minaccia e adottino le misure necessarie per garantire la nostra sovranità digitale*".

L'attacco informatico all'emittente TV Nine Network

Non solo il Parlamento. La notizia si è infatti diffusa in concomitanza dell'attacco hacker contro l'emittente televisiva australiana **Nine Network**, che ha portato all'interruzione di alcuni programmi nella giornata di domenica.

L'attacco è avvenuto quando il programma ***Weekend Today*** di Nine

Network non è andato in onda nella sua solita fascia oraria domenicale dalle 7:00 alle 13:00. Nine Entertainment, proprietario dei giornali come **Sydney Morning Herald** e **Age**, ha confermato domenica sera che stava rispondendo a *"un attacco informatico ai propri sistemi".*

"I nostri team IT lavorano 24 ore su 24 per ripristinare completamente i nostri sistemi che hanno interessato principalmente le nostre unità aziendali Broadcast e Corporate. I sistemi di pubblicazione e radio continuano ad essere operativi ", ha affermato la società in una nota.

Anche se ancora non è chiaro se esista qualche collegamento tra l'attacco al Parlamento e quello a Nine Network, i media locali hanno riferito che l'incidente è stato il più grande attacco informatico che abbia mai colpito una società di broadcasting australiana.

Attacco hacker all'Australia: il sospetto della Cina

I criminali informatici spesso prendono di mira i parlamenti e le legislazioni nazionali per ottenere l'accesso alle e-mail dei membri. Fonti governative temono che il sistema informatico parlamentare australiano sia sotto attacco da parte di un attore straniero, che potrebbe essere la Cina (già accusata dall'intelligence finlandese all'inizio di questo mese).

Già in passato funzionari dell'intelligence australiana hanno incolpato il Ministero della sicurezza statale cinese per aver violato il parlamento australiano e diversi partiti politici nel 2019 nonostante sia le società australiane che gli enti governativi hanno bloccato una serie di attacchi informatici nel corso dell'ultimo anno.

https://www.key4biz.it/australia-attacco-informatico-al-parlam

ento-sospettata-la-cina/353055/

Cyber attacchi prima minaccia per il 27% delle imprese italiane



La **sicurezza informatica** è sempre più al centro delle preoccupazioni delle **imprese italiane** che, in aggiunta ai cyber attacchi, di per sé temibili per danni e conseguenze non solo di natura economica, vedono come criticità serie anche la disinformazione e le tensioni crescenti in seno all'Unione europea.

Imprese italiane e cyber attacchi

Secondo dati diffusi in occasione del 32° Workshop Ambrosetti e riportati dal Sole 24 Ore, **il 27% delle imprese è**

preoccupata per gli attacchi informatici e le fake news.

Le difficoltà politiche e regolatorie dell'Unione preoccupano il 25,4% degli imprenditori che hanno risposto con il televoto al sondaggio.

Il mondo delle imprese vorrebbe che le istituzioni si impegnassero maggiormente per migliorare le condizioni generali del mondo del lavoro, che fossero più rapide nel prendere decisioni e nel garantire risorse finanziarie lì dove ce n'è bisogno, invece di alimentare tensioni e rimandare il confronto su problemi globali sempre più minacciosi.

Al contrario, subiscono in maniera negativa la **guerra tecnologica tra Cina e Stati Uniti** (15,9%), l'accumularsi degli **allarmi sul clima rimasti inascoltati** (11,1%), la **crisi tra Mosca, Europa e Stati Uniti** (9,5%), la **sicurezza nel Mediterraneo** (4,8%), l'attrito tra Donald Trump e Joe Biden in occasioni della tornata elettorale americana (3,5%), il terrorismo internazionale e la rinnovata conflittualità tra India e Cina in Asia.

Anche l'industria nel mirino del crimine informatico

Le paure espresse dalle imprese, soprattutto quelle relative ai cyber attacchi, sono di fatto una realtà anche per il mondo industriale. Qui le conseguenze, ovviamente, sono molto più pesanti, sia in termini di danni legati alle interruzioni della produzione, sia per le perdite finanziarie complessive.

In una recente indagine di Kaspersky, condotta a livello globale, si stima che nel secondo semestre del 2020 siano stati **vittima di attacchi informatici il 33,4% dei sistemi di controllo industriale** (o Ics), un dato in lieve crescita di quasi il +1% rispetto ai primi sei mesi dell'anno.

Su tali sistemi sono state bloccate minacce appartenenti a 5.365 famiglie diverse di malware, con un **aumento del +30% rispetto ai primi sei mesi del 2020**.

Tipologia di attacchi

Le minacce più importanti sono state *backdoo*r (pericolosi trojan che ottengono il controllo remoto sul dispositivo infetto), *spyware* (programmi dannosi progettati per rubare dati), altri tipi di *trojan* e *script* e documenti dannosi.

In Italia l'incremento è stato del 27,3%, per un aumento di +3,2 punti percentuali. Tra i settori più colpiti troviamo quello dell'ingegneria e dell'integrazione di Ics, con una crescita di quasi il +8%, seguito da *building automation* e *oil&gas*, con una crescita rispettivamente del +7% e del +6,2%.

Nel mondo, la percentuale di computer Ics attaccati è aumentata nel 62%.

https://www.key4biz.it/cyber-attacchi-prima-minaccia-per-il-27-delle-imprese-italiane/352727/

'Next Generation Cybersecurity SOC: La protezione delle infrastrutture critiche a

difesa del business Made in Italy’. Live Talk domani alle 11,00

Come è cambiato lo scenario della cybersecurity nell’ultimo anno?

In che modo la pandemia ha influito sull’attività del cybercrime?

Le aziende si sono attrezzate per rispondere alle nuove minacce figlie del lockdown?

Sono questi alcuni degli argomenti che saranno affrontati durante l’executive webinar organizzato da Cybersecurity Italia, che si terrà venerdì 26 marzo a partire dalle 11,00 e battezzato ***“Next Generation Cybersecurity SOC: La protezione delle infrastrutture critiche a difesa del business Made in Italy”.***

[embedded content]

Il contesto

Il numero record di Attacchi informatici registrati durante la pandemia a livello globale, con un incremento del 20% delle minacce cibernetiche portate nel 2020 nel nostro Paese contro asset rilevanti, getta una luce estremamente preoccupante sulla sicurezza IT nazionale. Un trend generale emerso dalla Relazione Annuale del **DIS**, che rispecchia un quadro in peggioramento nel mondo, con ben 1.821 attacchi gravi registrati nel 2020 che hanno provocato pesanti impatti con risvolti politici, sociali, economici e geopolitici **(Rapporto**

CLUSIT). In media, si tratta di 156 attacchi gravi al mese nel 2020, in aumento rispetto ai 139 del 2019.

Il Cybercrime ha rappresentato l'81% degli attacchi gravi a livello globale, mentre il Cyber Espionage costituisce il 14% delle minacce rilevate. Il 10% degli attacchi portati a termine da fine gennaio 2019 è stato a tema COVID-19, il 55% dei quali al fine di estorcere denaro.

Infrastrutture critiche

*Tutte l*e infrastrutture critiche che erogano servizi che implicano una forte attenzione alla riservatezza dei dati personali e finanziari sono interessate, si tratti di PMI, di aziende del settore sanitario, assicurativo, medico, incluse ovviamente le Pubbliche Amministrazioni.

Risulta vieppiù fondamentale garantire la protezione dei dati e quindi del business, attraverso un costante ed approfondito monitoraggio degli eventi, anche attraverso sistemi di intelligenza artificiale in grado di contrastare gli attacchi informatici, sempre però in concomitanza col supporto degli analisti. Qualunque genere di attività, dalle grandi aziende alle PMI, ha bisogno di uno scudo affidabile.

Durante il live talk i relatori interverranno portando la loro visione ed esperienza, suggerendo approcci utili alla gestione di un contesto così critico, per la tutela del business ma infine della comunità tutta.

Bozza di agenda:

Modera: **Arturo Di Corinto**

Relatori (in ordine alfabetico):

– **Michele Colajanni**, Dip. di Informatica – Scienza e Ingegneria, Università degli Studi di Bologna.

– **Luigi Maracino**, General Manager di Atlantica – Cybernext

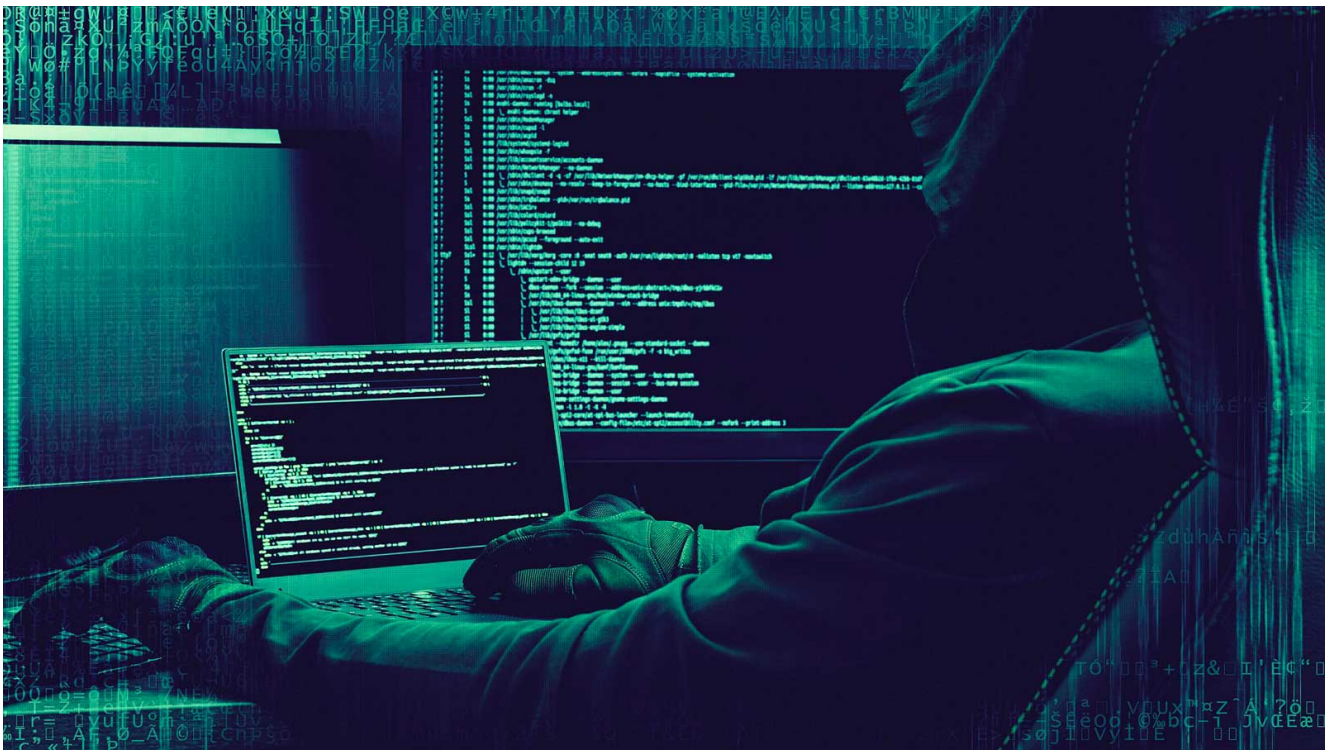
– **Stefano Mele**, Avvocato specializzato in Diritto delle tecnologie, Privacy e Cybersecurity

– **Yuri Giuseppe Rassega**, Chief Information Security Officer, Enel

– **Luigi Rebuffi**, Secretary General at European Cyber Security Organisation (ECSO)

https://www.key4biz.it/next-generation-cybersecurity-soc-la-protezione-delle-infrastrutture-critiche-a-difesa-del-business-made-in-italy-live-talk-domani-alle-1100/352272/

PNRR e cybersecurity, Colao: “Investiremo in personale e nuove strutture”



Più risorse per chi protegge lo Stato e cittadini e per chi sviluppa software, potenziando in maniera organica tutta la filiera della cybersecurity per garantire che all'aumento del tasso di digitalizzazione del Paese faccia seguito un aumento della nostra sicurezza.

Sono queste in sintesi le proposte dettate oggi dal ministro per l'Innovazione tecnologica e la Transizione digitale, **Vittorio Colao**, in audizione presso le commissioni riunite Bilancio, Lavori pubblici, Politiche Ue e Trasporti del Senato sul PNRR.

"L'aumento delle nostre capacità difensive passerà, ha dichiarato Colao, *da un rafforzamento della sicurezza cibernetica di asset strategici con la piena attuazione della disciplina in materia di "Perimetro di Sicurezza Nazionale Cibernetica" per la quale dovremo rafforzare sia le strutture preposte sia le amministrazioni pubbliche e private più sensibili ed esposte. Dovremo inoltre,"* ha aggiunto, *"rafforzare la capacità tecniche per una valutazione e audit continuo della sicurezza degli apparati elettronici e delle applicazioni utilizzate per l'erogazione di servizi*

critici da parte di soggetti che esercitano una funzione essenziale”.

Un altro passo importante per il ministro Colao riguarda potenziare le capacità di risposta agli attacchi informatici da parte del settore pubblico e del privato, con investimenti per chi sviluppa software in modo da salvaguardare i dati degli italiani perché ha dichiarato *“serve andare sempre più in profondità su codici software e architetture microelettroniche per verificarne l’integrità e l’eventuale vulnerabilità. Sarà anche importante potenziare le capacità di risposta e intervento del pubblico e delle imprese per gestire i rischi di attacchi cibernetici, soprattutto in relazione a dati dei cittadini”.*

Infine non mancano i riferimenti agli investimenti in personale specializzato e in strutture adatte per la prevenzione del crimine informatico. Il ministro ha concluso dichiarando di “*investire nuovo personale e strutture sia nelle aree di pubblica sicurezza e polizia giudiziaria dedicate alla prevenzione e investigazione del cybercrimine a protezione dei cittadini, sia in quelle dei comparti preposti a difendere il Paese da minacce cibernetiche. Anche e soprattutto in quest’area il raccordo con le iniziative Europee e alleate è essenziale per massimizzare la protezione degli interessi comuni dei cittadini e delle imprese”.*

https://www.key4biz.it/pnrr-e-cybersecurity-colao-investiremo-in-personale-e-nuove-strutture/351031/

‘Next Generation

Cybersecurity SOC: La protezione delle infrastrutture critiche a difesa del business Made in Italy’. Live Talk il 26 marzo alle 11,00

Come è cambiato lo scenario della cybersecurity nell’ultimo anno?

In che modo la pandemia ha influito sull’attività del cybercrime?

Le aziende si sono attrezzate per rispondere alle nuove minacce figlie del lockdown?

Sono questi alcuni degli argomenti che saranno affrontati durante l’executive webinar organizzato da Cybersecurity Italia, che si terrà venerdì 26 marzo a partire dalle 11,00 e battezzato ***“Next Generation Cybersecurity SOC: La protezione delle infrastrutture critiche a difesa del business Made in Italy”.***

Il contesto

Il numero record di Attacchi informatici registrati durante la pandemia a livello globale, con un incremento del 20% delle minacce cibernetiche portate nel 2020 nel nostro Paese contro asset rilevanti, getta una luce estremamente preoccupante

sulla sicurezza IT nazionale. Un trend generale emerso dalla Relazione Annuale del **DIS**, che rispecchia un quadro in peggioramento nel mondo, con ben 1.821 attacchi gravi registrati nel 2020 che hanno provocato pesanti impatti con risvolti politici, sociali, economici e geopolitici **(Rapporto CLUSIT)**. In media, si tratta di 156 attacchi gravi al mese nel 2020, in aumento rispetto ai 139 del 2019.

Il Cybercrime ha rappresentato l'81% degli attacchi gravi a livello globale, mentre il Cyber Espionage costituisce il 14% delle minacce rilevate. Il 10% degli attacchi portati a termine da fine gennaio 2019 è stato a tema COVID-19, il 55% dei quali al fine di estorcere denaro.

Infrastrutture critiche

*Tutte l*e infrastrutture critiche che erogano servizi che implicano una forte attenzione alla riservatezza dei dati personali e finanziari sono interessate, si tratti di PMI, di aziende del settore sanitario, assicurativo, medico, incluse ovviamente le Pubbliche Amministrazioni.

Risulta vieppiù fondamentale garantire la protezione dei dati e quindi del business, attraverso un costante ed approfondito monitoraggio degli eventi, anche attraverso sistemi di intelligenza artificiale in grado di contrastare gli attacchi informatici, sempre però in concomitanza col supporto degli analisti. Qualunque genere di attività, dalle grandi aziende alle PMI, ha bisogno di uno scudo affidabile.

Durante il live talk i relatori interverranno portando la loro visione ed esperienza, suggerendo approcci utili alla gestione di un contesto così critico, per la tutela del business ma infine della comunità tutta.

Bozza di agenda:

Modera: **Arturo Di Corinto**

Relatori (in ordine alfabetico):

– **Michele Colajanni**, Dip. di Informatica – Scienza e Ingegneria, Università degli Studi di Bologna.

– **Luigi Maracino**, General Manager di Atlantica – Cybernext

– **Stefano Mele**, Avvocato specializzato in Diritto delle tecnologie, Privacy e Cybersecurity

– **Yuri Giuseppe Rassega**, Chief Information Security Officer, Enel

– **Luigi Rebuffi**, Secretary General at European Cyber Security Organisation (ECSO)

https://www.key4biz.it/next-generation-cybersecurity-soc-la-protezione-delle-infrastrutture-critiche-a-difesa-del-business-made-in-italy-live-talk-il-26-marzo-alle-1100/350434/

Azienda nel mirino dei cybercrime? Il SOC di Atlantica Digital per proteggere il business e la

reputazione

Attacchi informatici record durante la pandemia a livello globale, con un incremento del 20% delle minacce cibernetiche portate nel 2020 nel nostro Paese contro asset rilevanti per la sicurezza nazionale.

Minacce in crescita con la pandemia

Un trend generale emerso dalla **Relazione Annuale del DIS**, che rispecchia un quadro in peggioramento nel mondo, con ben 1.821 attacchi gravi registrati nel 2020 che hanno provocato impatti gravi con risvolti politici, sociali, economici e geopolitici **(Rapporto CLUSIT)**. In media, si tratta di 156 attacchi gravi al mese nel 2020, in aumento rispetto ai 139 del 2019.

Il *Cybercrime* ha rappresentato l'81% degli attacchi gravi a livello globale, mentre il *Cyber Espionage* costituisce il 14% delle minacce rilevate. Il 10% degli attacchi portati a termine da fine gennaio 2019 è stato a tema COVID-19, il 55% dei quali al fine di estorcere denaro.



Il Next Generation SOC

E’ in questo difficile contesto che opera Atlantica Digital, la storica azienda attiva da oltre 30 anni nell’ICT specializzata nella progettazione e gestione di soluzioni digitali. In particolare, per contrastare la minaccia crescente del Cybercrime, Atlantica Digital ha realizzato mediante la società controllata CYBERNEXT un **CSOC (Cyber Security Operation Center)** di ultima generazione, gestito da una struttura dedicata di specialisti che si trova nel cuore di Roma.

Investimento importante

“Il Next Generation SOC è uno dei nostri investimenti più importanti che ci pone all’avanguardia in un settore estremamente critico e delicato per tutte le organizzazioni sia pubbliche che private – ha detto **Pierre Levy**, Presidente e Amministratore delegato di Atlantica Digital – *Cybernext garantisce la protezione dei dati e quindi il business dei nostri clienti con un costante ed approfondito monitoraggio degli eventi, anche attraverso sistemi di intelligenza artificiale, in grado di contrastare gli attacchi informatici grazie alla capacità dei nostri analisti. Qualunque genere di attività, dalle grandi aziende alle PMI, ha bisogno di questo scudo affidabile ed innovativo”.*

AI e Machine Learning per l’extended IT

Il Next Generation SOC di Atlantica Digital utilizza le capacità dell’Intelligenza Artificiale e del Machine Learning per attività di *detection* e *response* in caso di attacchi, ma soprattutto in chiave preventiva. Queste funzionalità sono state ampliate in ambito di extended IT che comprendono anche il mondo OT e IoT. Atlantica Digital lavora per la sicurezza

digitale ma anche fisica dei suoi clienti, proteggendo infrastrutture critiche e dati aziendali di grandi e piccole aziende.

Grandi aziende e PMI

"Siamo attivi nel mondo delle Grandi Aziende, ma sempre più ci rivolgiamo anche alla variegata galassia delle PMI attive in diversi Vertical – ha aggiunto Pierre Levy – *le nostre soluzioni sono disegnate per tutte le aziende che hanno nel dato il loro valore e il principale focus di business".* In sintesi, tutte le infrastrutture critiche che erogano servizi che implicano una forte attenzione alla riservatezza dei dati personali e finanziari. Ad esempio, aziende del settore sanitario, assicurativo, medico senza dimenticare le Pubbliche Amministrazioni.

Atlantica Digital è in possesso delle certificazione Iso9001 e 27001 e ancora della seguenti:

- **ISO/IEC 27017 è una linea guida che definisce controlli avanzati sia per fornitori, sia per i clienti di servizi cloud.** Chiarisce ruoli e responsabilità dei diversi attori in ambito cloud con l'obiettivo di garantire che i dati conservati in cloud computing siano sicuri e protetti.
- **ISO/IEC 27018** – *Codice di condotta per la protezione delle PII (Personally Identifiable information) nei servizi di public cloud per i cloud provider-* **è una linea guida per i fornitori di servizi cloud pubblici che vogliono migliorare la gestione dei dati personali.** L'obiettivo di questo standard è quello di fornire una modalità strutturata, basata sul privacy by design, per far fronte alle principali questioni giuridiche, sia di natura legale che contrattuale, legate alla gestione dei dati personali in infrastrutture informatiche distribuite seguendo il

modello del cloud pubblico.
- **ISO/IEC 27035** – Security incident management

Il profilo di Atlantica Digital

Atlantica Digital progetta e realizza da oltre 30 anni soluzioni software altamente innovative e infrastrutture informatiche solide, scalabili e sicure per un mercato in continua evoluzione.

Atlantica Digital, che opera per grandi imprese nelle aree Telco, Industria, Trasporti, Energia e Pubbliche Amministrazioni, è leader nei progetti di **ICT transformation**, di **virtualizzazione** e consolidamento, di **business continuity** e **disaster recovery**.

Sedi a Roma e Milano

Presente sul territorio nazionale con sedi a Roma e Milano e all'estero con una rappresentanza a Dubai, Atlantica Digital ha un organico di 200 dipendenti e un piano industriale incentrato sulle aree di maggior sviluppo quali la **Trasformazione Digitale**, la **Cyber Security** e lo **Smart Metering** con particolare attenzione al settore idrico in forte evoluzione.

Attenta alle esigenze del Mercato, **Atlantica Digital** ha sviluppato soluzioni e prodotti innovativi in ambito **Smart Metering**, **Digital Solution**, **Machine Learning**, **IoT**, **Cyber Security** e servizi gestiti di **Next Generation SOC** con la nascita, nel luglio 2020, di **Atlantica Cybernext.**

Atlantica Cybernext

Atlantic Cybernext è la società del gruppo che ha lo scopo di assistere e proteggere i Clienti, mediante il suo innovativo

Cyber Security Operation Center, dagli **attacchi cibernetici.**

Atlantica dedica inoltre molte risorse alla **ricerca**, alla **crescita professionale dei dipendenti**, dando spazio alle loro idee, così da fare nascere, per passione e capacità, molti progetti che evidenziano non solo le doti tecniche del personale ma anche l'indole all'innovazione che, da sempre, ha contraddistinto l'azienda.

Contatti:

Ufficio Stampa Now Italia

ufficiostampa@nowitalia.it

https://www.key4biz.it/azienda-nel-mirino-dei-cybercrime-il-soc-di-atlantica-digital-per-proteggere-il-business-e-la-reputazione/349843/

Phishing anche sui siti sicuri https. Clicca sul lucchetto prima di cedere dati o fare acquisti online

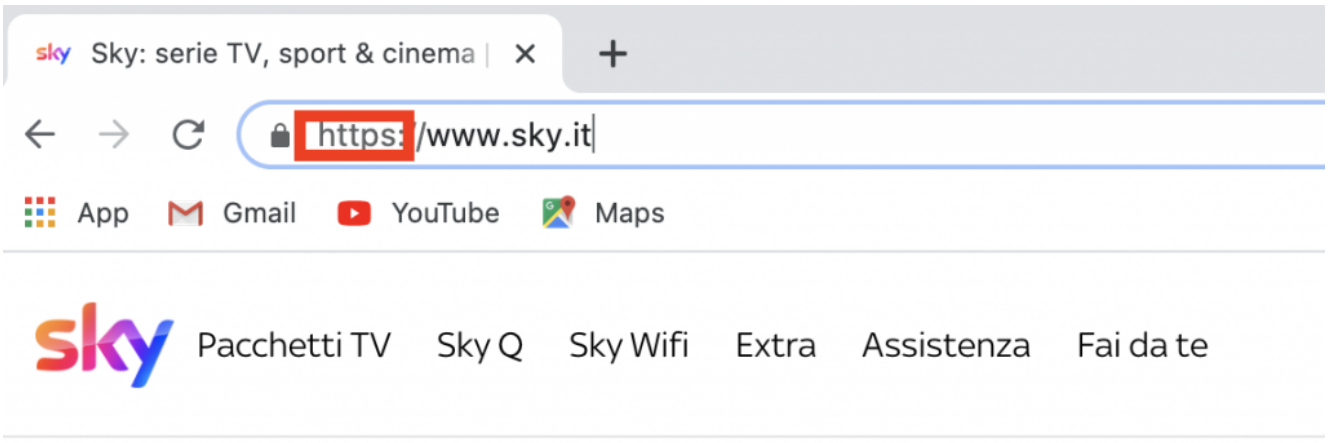
Un sito in https è sicuro, ma non è detto che sia anche al sicuro dai criminali informatici. Infatti, è possibile abboccare a phishing o essere vittime di malware anche su un sito con il protocollo https (hypertext transfer protocol secure), che garantisce sì una connessione protetta, ma non certifica chi c'è "dietro": allora come avere la garanzia di essere sul sito reale della propria banca, di una fintech, di

un eCommerce, di una società privata o ente pubblico?

Come sapere se un sito web è sicuro/protetto

La prima cosa da fare, per sapere se sei sul sito reale e non su uno fraudolento, a quest'ultimo si può giungere cliccando un link contenuto in un'email o SMS phishing o perché si digita il dominio con errori di battitura, è **guardare, con attenzione, l'url del sito web**.

Se inizia con "**https**" invece di "**http**", significa che il sito è **protetto** utilizzando un **certificato TLS/SSL**, che mette al sicuro i tuoi dati mentre vengono trasferiti dal tuo browser al server del sito web. Quando visiti un sito web codificato, per esempio per operazioni di banca online o eCommerce, il browser controlla se il certificato del sito è valido. Se non lo è, ti avvisa. In questo modo vengono protette le informazioni di login, i numeri di carta di credito, gli indirizzi e ogni altro dato riservato.



Che cos'è il protocollo SSL

Il Secure Socket Layer (**SSL**) e il suo successore Transport Layer Security (**TLS**) sono protocolli crittografici che permettono una comunicazione sicura sulle reti TCP/IP, come i

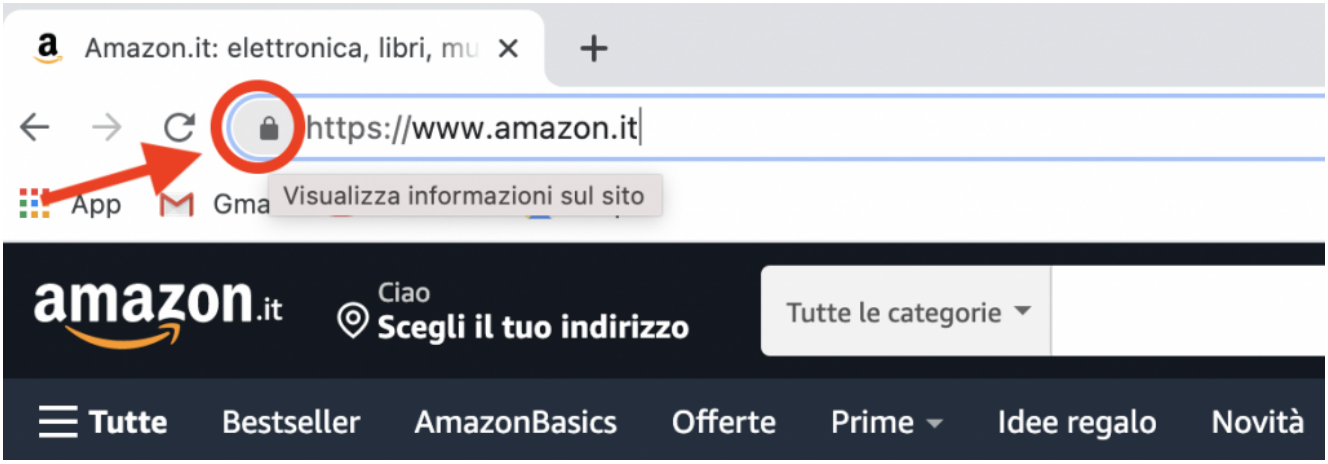
siti web, fornendo: autenticazione, crittografia e integrità dei dati. Il protocollo TLS/SSL risulta essere, dunque, un mezzo estremamente potente per la conduzione di transazioni online, autenticate e cifrate.

I certificati non sono tutti uguali

Tuttavia, i certificati TLS/SSL non sono tutti uguali: esistono diversi livelli di convalida e alcuni di essi sono più facili da superare rispetto ad altri.

Il livello di convalida più basso, Domain Validation (DV), verifica semplicemente la proprietà del dominio e non effettua un controllo sull'identità e legittimità dell'organizzazione che richiede il certificato. In altre parole, se hai acquistato il dominio **"amaz0n.com"** e hai richiesto un certificato, riceverai il certificato perché sei il proprietario del dominio. I browser mostreranno anche un piccolo lucchetto nella barra degli indirizzi per mostrare che il sito è protetto con la crittografia TLS/SSL. Ma, solo il lucchetto ti dirà se il sito ha la crittografia o meno ed occorre guardare oltre il lucchetto, cliccarci, per leggere gli indicatori di fiducia più elevati che garantiscono all'utente di essere sul sito web giusto.

Cosa c'è dietro il lucchetto



Prima di cedere dati personali o fare acquisti online con

carta di credito, bancomat, prepagata o altro, è necessario cliccare sul lucchetto che si visualizza **all'interno o accanto alla barra degli indirizzi del browser** per andare a caccia di indizi sull'identità e visibilità dell'azienda del sito. Solo così è possibile prendere atto di una serie completa di operazioni di sicurezza eseguita con successo.

Riccardo Cazzola, ceo Trust Italia: "*Solo cliccando sul lucchetto si visualizzano le informazioni certificate sull'identità dell'organizzazione che gestisce il sito*"

"La presenza del lucchetto nella barra degli indirizzi ci garantisce 'semplicemente' che il certificato sia valido, firmato da una Certification Authority verificata e che la connessione sia crittografata e sicura, ma è solo cliccando sul lucchetto che si ottengono tante informazioni relative al sito web che stiamo visitando, al tipo di crittografia in uso nella connessione https, ma soprattutto acquisiamo informazioni certificate sull'identità dell'organizzazione che gestisce il sito", ci spiega **Riccardo Cazzola**, ceo **Trust Italia**, azienda italiana specializzata dal 2000 nella web security.

"Infatti", continua Cazzola, *"le aziende e le organizzazioni che vogliono esporre la propria identità scelgono certificati di tipo OV (Organizational Validated) o, meglio ancora, di tipo EV (Extended Validation) che, in forza di una più approfondita procedura di verifica da parte della Certification Authority, espongono con più dettaglio e maggiore risalto i dati identificativi del proprietario del sito".*

"Al contrario", conclude il ceo di Trust Italia, *"i certificati DV (Domain Validated) si limitano a confermare solo che si sta visitando una pagina che riferisce al dominio riportato nel certificato stesso."*



Il certificato più sicuro? Extended Validation: certifica l’identità e la legittimità dell’azienda proprietaria del sito. L’utente è sul sito reale, i dati sono al sicuro e sa a chi li sta fornendo

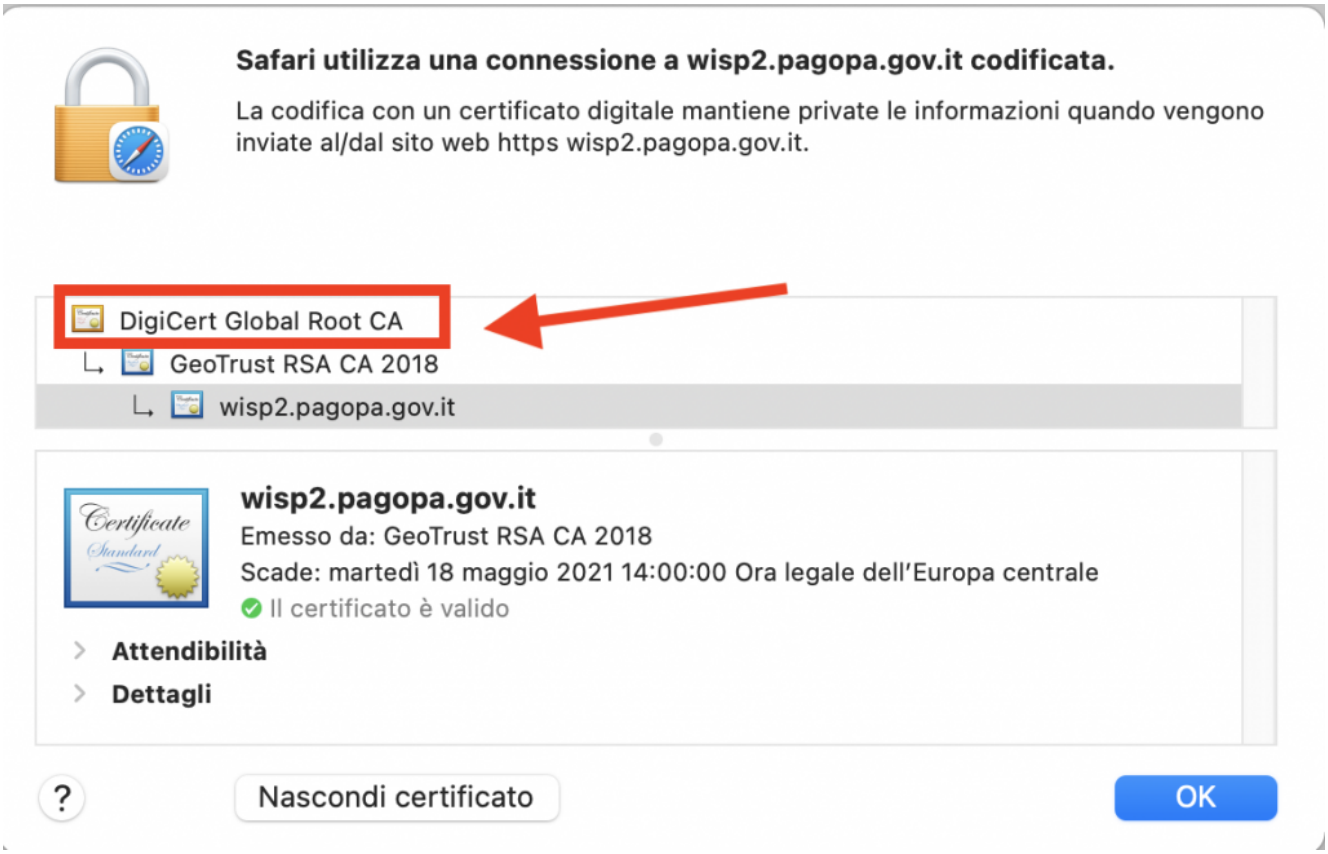
Qual è la scelta più sicura ed affidabile per le pagine di online banking, di eCommerce, una pagina di login o di pagamenti digitali di una società pubblica o privata?
Il più alto livello di convalida e con rigorosi standard è l’Extended Validation (EV), perché certifica l’identità e la legittimità dell’azienda proprietaria del sito. L’utente è sul sito reale, i dati sono al sicuro e sa a chi li sta fornendo. Questo legame tra il certificato e il nome di dominio offre agli utenti la garanzia di interagire con il sito web di un’organizzazione autorizzata e legalmente riconosciuta.

Infatti l’**Extended Validation:**

- Garantisce la cifratura delle comunicazioni https.
- Verifica attraverso un controllo stringente l’identità aziendale.
- Rende visibile nei dettagli del lucchetto il nome

dell'azienda, indirizzo fisico e numero di telefono. Tutte informazioni assenti nei certificati TLS/SSL usati per i siti fraudolenti.
- Viene emesso in massimo 3 giorni.

I certificati digitali sono firmati, di norma, da una terza parte affidabile e indipendente che ne garantisce la validità: si chiama Autorità di Certificazione o Certification Authority (CA). **DigiCert** è la più riconosciuta CA del mondo.



Dean Coclin (DigiCert): *"I consumatori devono essere certi di essere sul sito web giusto"*

"L'identità sul web continua ad essere importante affinché i consumatori siano certi di essere sul sito web corretto. I certificati SSL EV giocano un ruolo importante dando agli utenti una elevata confidenza sulla autenticità del sito che stanno visitando. I browser hanno spostato la visualizzazione dell'EV dietro il lucchetto quindi è importante che gli utenti

guardino oltre il lucchetto e ci clicchino su per vedere chi è il proprietario del sito web”, osserva **Dean Coclin**, Sr Director Business Development di DigiCert Inc.

Dietro il lucchetto c’è di più

Dunque, un sito in https garantisce sì la cifratura delle comunicazioni, ma l’utente non ha la certezza di chi ci sia “dietro”, se la società o l’ente a cui pensa di effettuare un bonifico o criminali informatici.
L’utente, prima di cedere dati o effettuare un acquisto online, deve valutare questi tre elementi se indicati nel certificato SSL:

- Crittografia.
- Identità digitale dell’azienda.
- Visibilità del brand.

Quindi, da oggi occhio alla url e a cosa c’è dietro il lucchetto.

https://www.key4biz.it/phishing-anche-sui-siti-sicuri-https-clicca-sul-lucchetto-prima-di-cedere-dati-o-fare-acquisti-online/349925/

Skill, la certificazione attraverso blockchain

Per il rilancio economico dell’Italia il premier **Mario Draghi** punta anche sulla formazione delle competenze, *“quelle chiave che sempre più permetteranno di fare carriera – digitali, tecnologiche e ambientali”*, ha sottolineato.

Come valutare e selezionare le migliori competenze?

Chi certifica le skill?

Un modo innovativo in grado di attestare in modo puntuale, incontrovertibile, la presenza a un corso di formazione e le competenze è la certificazione attraverso piattaforme **blockchain**.

"Il certificato digitale che attesti le presenze e/o le competenze acquisite dai partecipanti ad un corso di formazione è una soluzione cui guardiamo con crescente interesse", ci spiega **Francesca Faggioni**, docente di Economia e Gestione delle Imprese all'**Università Roma Tre**, nonché direttore del corso di perfezionamento in *"Blockchain Technology and Management".*

Faggioni utilizza la piattaforma blockchain di **Lirax**, per la parte laboratoriale del corso di perfezionamento, "*per certificare la presenza effettiva degli studenti durante il laboratorio e per costruire la loro identità digitale*".

Con le certificazioni digitali si ha e-portfolio sempre a portata di mano

"*Le certificazioni digitali*", continua Faggioni, "*sono attestazioni di competenze verificabili in modo digitale (machine-readable), sicuro (integrità) e rapido (in tempo reale); sono generalmente utili per tutti i soggetti della formazione. In sostanza, di un corso di qualsiasi tipo è possibile lasciare una traccia attraverso piattaforme in grado di certificare le skill acquisite e di raccoglierle anche in un e-portfolio, o Libretto delle competenze, come una sorta di CV digitale, sempre a portata di mano e condivisibile".*

Per cui”, ha concluso Francesca Faggioni,*“intravedo tantissime potenzialità di questa tecnologia per la certificazione delle competenze, soprattutto in questi settori dove è necessario identificare in modo certo l’emittente; rendere immutabili le credenziali; identificare in modo certo il learner; consentire una verifica disintermediata; non diffondere i dati sensibili del learner pur attestandone le credenziali ed, infine, assicurare regolarità e trasparenza rispetto all’effettivo svolgimento del corso attraverso la credibilità dell’emittente”.*



Blockchain di Lirax: una certificazione anche social

La certificazione viene emessa, attraverso una piattaforma blockchain, da una Università o da un ente formatore, in qualità di erogatori del corso e quindi come unici soggetti emittenti (issuers), con tre fattori abilitanti: identità,

competenza e tempo di frequenza del partecipante.

“È possibile condividere sui social la certificazione attraverso il proprio badge conseguito partecipando al webinar. Grazie a questo importante strumento, in modo semplice ed efficace, il tempo trascorso online trova un riscontro oggettivo in una attestazione ufficiale, trasparente, registrata in modo indelebile all’interno del ‘libretto’ personale in Blockchain, i cui estremi sono stati tokenizzati con tecnologia Takamaka”, ha osservato **Alessadro Civati**, ceo Lirax – Blockchain&AI Trust Provider.

Per ulteriori informazioni su come adottare il libretto delle competenze e su come condividere il badge in blockchain clicca qui.

https://www.key4biz.it/skill-la-certificazione-attraverso-blockchain/349923/

OVH, incendio nel data center di Strasburgo. Problemi per migliaia di siti (anche italiani)



Una gravissimo incendio ha colpito la notte scorsa 3 delle 4 aree del data center di Strasburgo di **OVH**, società di web hosting francese. Il datacenter è uno dei più grandi d'Europa.

L'incendio, che si è propagato verso le 3 del mattino, è stato domato solo dopo 4 ore dagli oltre 100 pompieri che sono intervenuti sul posto. Fortunatamente non ci sono state vittime.

> *#Strasbourg Un bâtiment de stockage de serveurs informatiques @OVHcloud_FR ravagé par un incendie #DNAinfos https://t.co/EuELb9Nux3 pic.twitter.com/MKlXDInhWP*
>
> *— Antoine Bonin (@abonin_DNA) March 10, 2021*

*"Tutti sono al sicuro. Le fiamme hanno distrutto **SBG2**. Una parte di **SBG1** è andata distrutta. I vigili del fuoco stanno proteggendo **SBG3**. Nessun impatto per SBG4"*, ha scritto su Twitter il CEO dell'azienda **Octave Klaba**.

“L’incendio è stato spento. I vigili del fuoco continuando a raffreddare gli edifici con l’acqua. Non abbiamo accesso al luogo. Questo è il motivo per cui SBG1, SBG3, SBG4 non verranno riavviati oggi”, ha scritto nel suo ultimo Tweet Klaba, non esprimendosi riguardo l’origine delle fiamme né quando (e se) i servizi saranno ripristinati.

> *We have a major incident on SBG2. The fire declared in the building. Firefighters were immediately on the scene but could not control the fire in SBG2. The whole site has been isolated which impacts all services in SGB1-4. We recommend to activate your Disaster Recovery Plan.*
>
> *— Octave Klaba (@olesovhcom) March 10, 2021*

Le conseguenze per i portali italiani

Le conseguenze dell’incendio di Strasburgo hanno colpito anche il nostro Paese dato che diversi portali italiani si affidano all’azienda francese per i propri servizi.

Nella mattinata di oggi infatti centinaia di siti internet sono in down o con gravi rallentamenti provocati dall’interruzione di corrente decisa dall’azienda dopo l’incendio.

Al momento non è ancora chiara l’entità del danno subìto, per quanto riguarda i dati persi dall’azienda.

OVH (acronimo di *On Vous Hébergeè, Noi vi ospitiamo*) è stata fondata a Roubaix nel 1998 da **Octave Klaba**. L’azienda che fornisce server dedicati, domini e servizi di telefonia, possiede 17 data center per un totale di 250mila server erogando servizi in 17 paesi tra cui Francia, Germania, Italia, Polonia, Spagna, Irlanda, Regno Unito, Finlandia e Canada.

https://www.key4biz.it/ovh-incendio-nel-data-center-di-strasburgo-problemi-per-migliaia-di-siti-anche-italiani/349421/