SEO and cybersecurity: Incorporating cybersecurity into your SEO strategy

30-second summary:

- Website security directly impacts the SEO performance of the website, as the non-compliance with the security requirements can cause low rankings or Google penalties.
- Blacklisting, malicious bots interfering with the crawling process, and spam attacks are among the main consequences of low website security.
- The “site not available” warning, the presence of strange JavaScript code, not working login credentials and frequent error messages can be the warning signs of a cyberattack on your website.
- Making security checks a part of your SEO strategy would help you create a website that is resistant to cybersecurity attacks.

Every site needs to be secure and there are no “too small” or “too unnecessary” sites for malicious attacks. Online businesses are fully centered on high search rankings for online reputation and profits. For this purpose, they often implement the most effective SEO tactics, from link building to great content marketing, to land up on the front page of Google search. Nevertheless, apart from delivering the best content to the users, Google is also aimed at making the internet a safe environment, hence placing importance on websites’ cybersecurity practices.

In fact, hacks may not only be destructive for your reputation but also for your site’s organic search performance. Hence, cybersecurity and SEO go hand in hand towards building a firm’s online reputation. If the website doesn’t mean the latest security compliance it can be blacklisted by Google, suffer from spam attacks or activities of malicious bots.

So we want to share effective advice on how to recognize the security vulnerabilities in time, how to integrate the security checks into your development strategy, why you should regularly scan your website, and how to protect your local networks.

Four main steps to improve website security

Security or the absence of security may seriously affect your SEO. We all know that the HTTP certificate is no longer a reliable way to secure the site and the HTTPS has, for the most part, become the poster boy of the security standard. In 2014, Google started to prioritize the sites with HTTPS in the search results.

Focusing on SEO and security will help your business to step on the steer of success. The struggle to improve the website’s ranking and keeping it cybersecurity is common for many companies so here what we suggest:

#1: Learn to recognize the earliest warning signs

Cyber attacks can cause malicious bots activity. Bots will always represent a part of your traffic but not all bots are harmless to the site’s security. Cybercriminals, however, launch bots to crawl sites in the search for vulnerable parts, data theft, or content crapping. Malicious bots use the same bandwidth as the “good” bots and normal visitors do. If your

server is a subject of repetitive tasks by malicious bots, it may lead to the server to stop serving pages.

Cybercriminals always rely on the website’s weak sides to hack it. Thus, it’s essential to stay ahead and pay attention to the following warning signs of cyberattacks that are supposed to make your inner radar shout. Cybercriminals can cause malicious bots activity.

Google Alerts and notifications

In case you received a Google alert notification or see a “Site not available” warning in search results, we have bad news. This is a sign that your website has been hacked. To confirm this fact, go to the Google Search Console, the Security Issues section, and look for the hacked URLs that Google has detected.

Presence of strange JavaScript code

The presence of a weird Java code in the source code of your website is a reliable alert sign. Javascript codes are often used by hackers to steal precious personal data like credit card details or passwords from your site. If you see any trace of strange-looking code, get rid of it immediately.

Your login credentials don’t work

Not hard to guess that something goes wrong when you enter the valid login info and get the “wrong password” notification. Your login credentials have been altered by cybercriminals.

You get frequent random popups or error messages

More than half of malicious attacks on websites are performed by “black” SEO’s who are aimed at improving their own site’s ranking. They target the sites with prominent search rankings and insert links or use Javascript to redirect users to their own malicious websites. SEO spamming allows scammers to use high-ranking websites in order to promote low-quality content

to low masses and, consequently, push their rankings. SEO spam has several negative impacts:

1. The site will get blacklisted by the search engine.
2. The site’s spam ranking may reduce the site’s ranking
3. The business reputation will get dramatically spoiled as visitors will see lots of spamming content.

Very often hackers use cross-site scripting or insert their own code into the source code of your website to bypass its security system. So if you get any kind of these notifications, don’t ignore them. It’s time to run a serious scan in order to discover the malicious software.

#2: Make security check a part of your developing strategy

If you ever become the subject of a cyber attack, financial losses are not the only concerning consequence. The compromised website may face a range of penalties by Google and distort the search results. When potential customers will look for your website, they will most probably first meet a warning page that will dissuade them from visiting your site. Consequently, it is essential to make cybersecurity a part of your SEO strategy.

Trusting Google alerts is a good piece of advice there’s more than that to be done. Learn to predict the possible threats and control the cybersecurity level. In addition to involving your team of IT-specialists, hire one more cybersecurity professional. Only a qualified specialist will help you discover the site’s vulnerabilities and elaborate on the cyber protection strategy for your eCommerce business.

#3: Use effective scanning tools

One more way to get rid of malicious intervention is by using a file malware scanner. The system looks at the website code

to check web pages for malware or strange PHP or HTML files on your server. The examples of scanners that can prevent your site from being penalized, blacklisted, and maintain your search engine rankings are Sucuri SiteCheck or Web Inspector.

In addition, open-source web analytics tools like AWStats can scan your log files for suspicious activity. This tool offers data on every bot that crawled your site, bandwidth consumed, last crawled date, and total hits, allowing you to detect malicious activity.

For example, a bot’s throughput does not exceed a few megabytes per month. If you face thousands of page hits from a single IP address within a short time period the available bandwidth will be limited.

Finally, use tools like Ahrefs and Majestic to check your backlink profile. They will not only improve your site’s SEO but also track down unnecessary backlinks from SEO spammers.

#4: Protect your security and privacy with VPN

No matter where you are in a remote area, at home, or office, local network security should be tightened under any circumstances. A large network is highly susceptible to human error, and the risks cannot be underestimated compared to a small network. All users need to ensure that they’re compliant with all standard security measures. Despite the time and place of their work, they must ensure that the traffic is controlled with the Web Application Firewall and the connections are encrypted with a stable VPN.

There are three main ways in which a VPN significantly increases the security of your website. First, it encrypts all the sensitive data, so hackers can’t access it. Second, VPN intercepts any malicious software or phishing attempts stopping them from infiltrating your system. And third, VPNs

are a must-have for companies having remote employees who might be accessing companies' systems using public hotspots as doing that without a VPN can lead to security vulnerabilities.

Today's market does not experience any shortage of quality VPN suppliers. So do your research and choose the VPN that would meet all of your business needs.

Conclusion

Internet security matters and it matters a lot. The security breach in your website's operation may cause dramatic damage to the eCommerce web site's reputation and income. Cybersecurity needs to become a part of your SEO strategy for all eCommerce companies that want to take the leading position on the market of online sales. Now when you know that safety is crucial within the web, it's time for the SEO and IT team to unite the forces and make up a reliable strategy that will raise the website's ranking and maintain the security of your site.

Connie Benton is a chief content writer, guest contributor, and enthusiastic blogger who helps B2B companies reach their audiences more effectively. You can find her on Twitter at @ConnieB34412379.

More about:

- *SEO and cybersecurity: Incorporating cybersecurity into your SEO strategy*

L’era Biden inizia con un cyber attacco al Governo americano. Dito puntato contro Mosca

È partita oggi, lunedì 14 dicembre 2020, la nuova presidenza Biden. Il Collegio elettorale nazionale si riunisce per ratificare ufficialmente l’elezione di **Joe Biden** a 46° Presidente degli Stati Uniti d’America.

Biden è il 46° Presidente USA

Chiusi tutti gli scrutini, respinte anche le cause intentate da alleati e legali di **Donald Trump**, ci si avvia a lasciarsi alle spalle una tornata elettorale americana tra le più combattute della storia e tra le più votate di sempre.

Biden ha vinto le presidenziali 2020 con oltre 81 milioni di voti, divenendo il Presidente più votato di sempre negli Stati Uniti. Trump, invece, sarà ricordato come lo sconfitto più votato di sempre, con oltre 74 milioni di voti.

Il **Collegio elettorale nazionale**, a questo punto, dovrà solo ufficializzare il dato finale dei grandi elettori: Biden 306

voti, Trump 232. Il prossimo 6 gennaio ci sarà la proclamazione del nuovo Presidente e vice Presidente USA (a cui seguirà l'ultimo atto rituale, l'*Inauguration Day* del 20 gennaio, giorno dell'insediamento alla Casa Bianca).

L'attacco hacker al Governo americano e la pista russa

Un giorno importante oggi per gli Stati Uniti e il mondo intero, macchiato però da un fatto molto grave, che getta ombre inquietanti sul futuro della più grande potenza economica e militare al mondo e sul futuro delle democrazie (ex) occidentali in generale.

Sabato il **Consiglio di sicurezza nazionale** si è riunito in via straordinaria proprio a causa di quello che i media americani non esitano a definire "*il più grave attacco informatico all'amministrazione USA da cinque anni a questa parte*".

I cyber attacchi hanno colpito il Dipartimento del Tesoro e il Dipartimento del Commercio, più altre Agenzie governative di massimo rilievo istituzionale. Dietro a tutto questo, secondo quanto riportato dal New York Times, ci potrebbe essere la Russia.

Breccia nei sistemi Microsoft e SolarWind

La breccia nel sistema di difesa è stata individuata in alcuni software della **NTIA**, la National Telecommunications and Information Administration, in particolare in **Microsoft Office 365**, superando il sistema di autenticazione.

Altra falla individuata dagli investigatori americani è negli aggiornamenti software rilasciati dalla società IT **SolarWind**, che fornisce servizi ad agenzie governative e Dipartimenti del

Governo, nonché all'intelligence USA e ai militari.

Secondo quanto riportata dalla Reuters, l'azienda ha dichiarato che gli upgrade in questione possano esser stati manomessi in effetti tra marzo e giugno 2020 in occasione di un grande attacco informatico, ben pianificato e mirato a degli specifici target.

Su quanto accaduto stanno investigando la ***Cybersecurity and Infrastructure Security Agency***, l'**FBI** e la ***National Security Agency*** (NSA).

Biden e il cattivo rapporto con Mosca

La NSA già ai primi di novembre, cioè in piena elezione presidenziale, aveva già denunciato il pericolo di attacchi informatici sponsorizzati da Mosca. Ma sono mesi che si parla di cyber attacchi su target governativi e politici.

Ora tutti i media americani, pur nell'incertezza generale, stanno puntando il dito contro la Russia: "*E' un attacco troppo grande, troppo ben congegnato, troppo mirato, dietro ci deve essere per forza una potenzia nazionale*", hanno detto alcune persone informate su fatti alla Reuters.

Il ministro degli Esteri russo, attraverso la pagina Facebook dell'Ambasciata russa negli Stati Uniti, ha respinto ogni accusa al mittente, bollando la vicenda come isteria mediatica e malafede di Washington con l'obiettivo di attaccare e mettere in cattiva luce Mosca.

Cold war

Nel tempo Biden non ha mai risparmiato frecciate a Mosca e parole a volte molto dure contro la Russia, i suoi interessi globali e la sua volontà di minare le basi delle democrazie

occidentali, americana compresa.

Ancora prima di vincere le elezioni presidenziali, ricorda un approfondimento dell'Istituto per gli Studi di Politica Internazionale, il candidato democratico aveva infatti dichiarato più volte che la sua posizione ufficiale nei riguardi di Mosca era ed è improntata ad un utilizzo pesante delle sanzioni, ad un'espansione e potenziamento progressivi della Nato, alla creazione di un fronte democratico internazionale finalizzato ad arginare l'azione della Russia nel mondo.

Tutti negli Stati Uniti si aspettano da Biden una nuova politica anti-russa, con un rafforzamento della presenza americana e della Nato nei Paesi a Est dell'Europa, tra cui Ucraina e Bielorussia, con un'inevitabile escalation della tensione, sia politica, sia economica, sia soprattutto militare.

L'attacco hacker denunciato da Washington in questi giorni sembra proprio inaugurare una nuova era politica, che tanto ricorda quella che un tempo si chiamava "guerra fredda" tra imperi.

> *L'era Biden inizia con un cyber attacco al Governo americano. Dito puntato contro Mosca*

Cybersecurity, l'Ue investe il 40% in meno degli Stati

Uniti. Il Report Enisa

Sappiamo bene ormai quanto sia importante investire nel settore della *cybersecurity*. Ogni anno nuovi Report ci avvertono della gravità delle minacce informatiche sempre in agguato e dei danni che sono in grado di causare ai singoli, alle imprese e alle stesse Istituzioni.

Bruxelles ne è cosciente, come lo sono gli Stati membri dell'Unione, eppure, secondo un **nuovo studio** pubblicato dalla *European union agency for cybersecurity* o **Enisa**, l'Agenzia europea per la sicurezza delle reti e dell'informazione, **gli investimenti pianificati in questo settore così strategico sono il 41% in meno rispetto agli Stati Uniti**.

Il Report dell'Enisa

Il documento, dal titolo "***Nis investments Report***", realizzato a partire da un'indagine che ha coinvolto **251 organizzazioni pubbliche e private di diversi Paesi, tra cui Italia, Germania, Spagna, Francia e Polonia**, ha infatti illustrato una situazione generale piuttosto critica in termini di implementazione della Direttiva NIS.

La **Direttiva europea Nis** (*Network and information security*), lo ricordiamo, è la normativa finalizzata a definire le misure

necessarie a conseguire un elevato livello di sicurezza delle reti e dei sistemi informativi, che secondo lo studio **è stata adottata e pianificata per l'implementazione solo dal 58,6% delle organizzazioni**.

Il 23,1% degli intervistati ha confermato di aver avviato programmi in tal senso, ma ancora in via di definizione e potenziamento, un 8% lo farà in futuro, un 10% non l'ha ancora neanche programmato.

Direttiva Nis ed elementi critici da superare

"*Da una parte abbiamo capito che la direttiva Nis è stata ed è un ottimo strumento per guidare gli investimenti in cybersecurity, ma dall'altra è evidente che esistono ancora lacune culturali e impedimenti di varia natura alla sua implementazione da parte delle aziende e non solo*", ha dichiarato Juhan Lepassaar, Executive Director dell'Enisa.

Lo studio rappresenta inoltre un valido punto di partenza per supportare il processo di revisione della direttiva Nis, che dovrebbe iniziare il 16 dicembre prossimo.

I punti chiave del confronto saranno, tra gli altri, la scarsa chiarezza negli obiettivi e negli strumenti (problema sollevato dal 35% degli intervistati) e il limitato sostegno finanziario dei singoli Stati (per il 22% dei partecipanti all'indagine).

Cybersecurity, attacchi e danni

Tra i dati messi in evidenza dall'Enisa ci sono i danni alle organizzazioni diretta conseguenza di cyber attacchi: nel 43% si è trattato di un impatto finanziario pari o superiore a 500 mila euro, mentre per il 15% anche superiore al milione di euro.

L’81% degli intervistati ha dichiarato di aver attivato sistemi di comunicazione diretta con le autorità nazionali per informare tempestivamente di ogni tipo di attacco informatico subito.

La spesa media in progetti di implementazione della Direttiva Nis a livello di imprese è di circa 175.000 euro, con il 42,7% delle organizzazioni interessate che stanziano risorse tra 100.000 e 250.000 euro.

> *Cybersecurity, l’Ue investe il 40% in meno degli Stati Uniti. Il Report Enisa*

Leonardo e il furto di dati, perché la cybersecurity non è solamente tecnologia

In questi giorni tra le notizie di cybersecurity più commentate c’è quella relativa al furto di dati del colosso della cyber difesa Leonardo, avvenuto nel corso di due anni (dal 2015 al 2017) ad opera – si legge – di un ex dipendente e un dirigente della società, accusati “*dei delitti di accesso abusivo a sistema informatico, intercettazione illecita di comunicazioni telematiche e trattamento illecito di dati personali e di depistaggio*”.

La notizia ha destato non poco scalpore tra gli addetti alla cybersecurity e non solo, considerate anche le possibili ripercussioni per il Paese. Credo però che il punto cruciale non sia quanto avvenuto, pur nella sua gravità. È accaduto e bisogna correre ai ripari, ma ormai non passa giorno senza che

ci sia una notizia su attacchi cyber o violazioni di dati. Ci stiamo abituando? Spero di no, perchè questo significherebbe rimanere inerti rispetto ad un futuro che si preannuncia sempre più complicato, e non solo dal punto di vista della sicurezza.

Indipendentemente dunque dal caso in questione e attendendo che le indagini facciano il loro corso, è doveroso fare delle riflessioni su come è stata affrontata fino ad oggi la cybersecurity, un tema che può davvero fare la differenza per qualsiasi Paese. La protezione di informazioni rilevanti e del *know-how* ha sempre rappresentato un obiettivo strategico, ancora di più oggi con la crescente digitalizzazione.

Due anni fa, ad inizio anno 2018 scrissi un articolo su Key4biz auspicando che la cybersecurity non fosse ridotta ad una sorta di farmaco da banco.

Siamo alle soglie del 2021 e i problemi della sicurezza informatica peggiorano, con numeri che crescono anno dopo anno, anche con attacchi altamente sofisticati dal punto di vista tecnico. Non lo dico io, lo raccontano report annuali sulla sicurezza informatica (es. quello italiano pubblicato dal **Clusit** o quello dell'americana **Verizon**) che puntualmente ci allertano sulla situazione catastrofica. Chiaramente, gli approcci risolutivi al 100% non sono fattibili, data la complessità del tema.

Ma è evidente che qualcosa non funziona. Un problema c'è, che però va oltre le colpe di qualcuno. Un problema di approccio e di visione strategica. Si continua a parlare di come le tecnologie sempre più innovative miglioreranno le nostre vite e daranno una svolta alla cybersecurity, ci si incensa quando si raggiunge qualche risultato, spesso effimero rispetto alla complessa realtà dei fatti.

Dal mio punto di vista ritengo innanzitutto che fino ad oggi sia prevalsa una strategia caratterizzata da una forte chiusura cognitiva (i cosiddetti paraocchi). Vale a dire ci si è concentrati quasi esclusivamente su aspetti puramente tecnologici, quando ormai è opinione sempre più diffusa che la cybersecurity è (soprattutto) un problema che riguarda le persone.

Le soluzioni tecnologiche, per quanto necessarie, arrivano fino ad un certo punto: tutto può essere blindato, ma poi arriva una minaccia interna e tutto crolla. Forse in questi casi un profiler esperto o un criminologo sono più efficaci di un ingegnere informatico! In fin dei conti, tecnologie e dispositivi sono funzionali al raggiungimento degli obiettivi, ma non agiscono da soli. In un modo o nell'altro l'elemento umano è sempre presente. Basti pensare agli attacchi ransomware il cui successo viene il più delle volte determinato dall'apertura di mail di phishing o di allegati per motivi squisitamente umani, dalla curiosità, all'empatia, alla mancanza di consapevolezza, e via dicendo.

È ormai palese che la cybersecurity non è più una questione solo tecnologica; purtroppo, per interessi e posizionamenti vari viene trattata come se lo fosse.

Basta con questa visione fallimentare, ripartiamo dal buon senso! Cominciamo a vederla in un'ottica multidisciplinare, in modo da riuscire a leggere gli scenari digitali in modo più articolato e ricerchiamo le competenze adeguate. Su questo punto, poi, è imperativo fare un ulteriore passo avanti. Le

competenze non si improvvisano, un tecnico informatico per quanto bravo non può essere delegato ad occuparsi del tema della consapevolezza digitale, perché questo richiede la conoscenza dei meccanismi umani e sociali relativi ai comportamenti. Non basta andare in aula e dire alle persone di non fare certe cose: ci stupiamo poi perché le persone continuano a commettere certi errori? Lavorare sul comportamento umano richiede ben altri tipi di competenze.

Parliamoci chiaro, c'è un problema di innovazione. Non tecnologica, ma di visione. Occorre ripartire dalle buone esperienze, svecchiare gli approcci, ridare "nuova linfa" alla cybersecurity, de-contaminandola anche da meccanismi non sempre meritocratici che a lungo andare producono seri danni. Inutile tentare di imitare le buone pratiche degli altri Paesi – correndo loro dietro quasi fosse una corsa ciclistica – se poi schemi e meccanismi proposti rimangono gli stessi.

Si, il cambiamento ci vuole. Ma cominciando dalle persone.

https://www.key4biz.it/leonardo-furto-di-dati-perche-la-cybersecurity-non-e-solamente-tecnologia/334143/

Computer Security Day: nel mondo spesi 167 miliardi in cybersecurity nel 2020, cresce l'impiego dell'IA

In tutto il mondo il 30 novembre di ogni anno viene celebrato il **Computer Security Day**, cioè la giornata mondiale per la sicurezza informatica del nostro computer e dei nostri dati.

Nata nel 988, la Giornata si pone l’obiettivo di promuovere tra gli utenti di rete di ogni età e status una maggiore consapevolezza riguardo i pericoli informatici insiti nella rete, tra cui la sottrazione illecita di informazioni sensibili.

Il mercato cybersecurity

Secondo uno studio pubblicato da Grand View Research, **la spesa globale in soluzioni cybersecurity entro la fine dell’anno supererà i 167 miliardi di dollari**.

Un risultato che è conseguenza diretta, in parte, dell’evolversi della pandemia, che ha letteralmente fatto esplodere l’ammontare dei dati prodotti da gestire.

Basti pensare alla **didattica a distanza**, allo ***smartworking*** e al boom dell’***ecommerce***. D’altronde, con l’aumento dell’attività online, si amplificano le minacce e gli attacchi della rete in tutti i settori chiave della nostra economia e della nostra società.

Da una parte serve che gli utenti si proteggano di più, adottando semplici azioni come scegliere password complesse, prestando attenzione a ciò che si scarica, facendo acquisti online sicuri.

Dall’altra, però, è compito delle aziende tutelare i dati personali dei propri utenti secondo il **GDPR**, ovvero il Regolamento Generale sulla Protezione dei Dati, entrato in vigore nel 2018.

Il mercato globale della Cyber Security comunque continuerà a crescere e il tasso di incremento sarà del +95,3% entro il 2027, per un valore stimato attorno ai 326.4 miliardi di dollari.

Applicazioni IA

Nel prossimo decennio 2020 – 2030, altra tecnologia fortemente legata alla sicurezza e la protezione informatica è l’**intelligenza artificiale** (IA).

Se l’impiego di **soluzioni IA per la cybersecurity** a livello globale hanno generato **investimenti** pari a 8,6 miliardi di dollari nel 2019, secondo uno studio Research and Markets, grazie ad un tasso di crescita medio annuo (Cagr) del +25,6%, tale spesa potrebbe ulteriormente aumentare arrivando a sfiorare i **102 miliardi di dollari entro la fine del prossimo decennio**.

Le **frodi** nei pagamenti online e i tentativi di rubare le **identità digitali** degli utenti di rete saranno le principali minacce, per un 55% del totale delle attività cyber criminali già oggi individuate.

L’intelligenza artificiale è infine utile per il contrasto a tali attacchi perché riduce i tempi di risposta, identifica co precisione le minacce, migliora e rende più efficaci le tecniche per distinguere gli attacchi che richiedono attenzione immediata.

https://www.key4biz.it/computer-security-day-nel-mondo-spesi-167-miliardi-in-cybersecurity-nel-2020-cresce-limpiego-dellia/333301/

Malware sLoad, in Italia nuova campagna malevola via PEC. L’allarme del CSIRT

È proprio di questa settimana la segnalazione fatta dal **CSIRT** in merito ad una doppia campagna orientata alla distribuzione del malware **sLoad** (noto anche come **StarsLord**), particolarmente insidiosa e che utilizza caselle di posta elettronica certificata (PEC) con un’elevata personalizzazione dei messaggi e l’impiego di allegati con alta capacità di evasione dalle protezioni antivirus.

Il malware Sload

SLoad è il nome di un software malevolo che funziona come downloader/dropper di malware. Le varie ricerche condotte mostrano che i criminal hacker diffondono sLoad tramite campagne malspam, ovvero attraverso gli allegati dannosi ai messaggi di posta elettronica. Questo malware concepito per i sistemi Windows è capace inoltre di raccogliere informazioni di sistema e inviarle a un server di comando e controllo remoto e presidiato (C2), dal quale riceve anche dei comandi. La comunicazione con il suo server C2 avviene, solitamente, per il tramite del servizio BITS che Windows utilizza invece legittimamente per inviare aggiornamenti del sistema operativo.

sLoad appartenendo alla famiglia dei PowerShell downloader è capace in particolare di carpire informazioni riguardo agli

elenchi dei processi in esecuzione e alla presenza di client di posta elettronica Microsoft Outlook oltreché acquisire screenshot, analizzare le cache DNS alla ricerca di domini specifici e eseguire il download di altri possibili payload come trojan o ransomware.

L'attacco rilevato in Italia

Secondo il CSIRT, le due campagne massive in corso e tra loro molto simili mirano a diffondere, da caselle PEC verosimilmente compromesse, il malware SLoad tramite un allegato .vbs ("Allegato_XXXXXXXXXXX") contenuto in archivi compressi con estensione .zip, dove la parte del nome variabile riporta, a seconda delle varianti, un codice numerico o il codice fiscale del destinatario.

Il messaggio e l'oggetto delle missive PEC

In tutti i casi, i messaggi dei campioni PEC esaminati risultano personalizzati con la ragione sociale ed i riferimenti di determinate aziende italiane (S.r.l. S.n.c) e sollecitano a prendere visione di una fattura insoluta emessa in formato elettronico o addirittura a stamparla su carta per l'efficacia fiscale. Anche l'oggetto è formulato in modo ingannevole. La prima parte variabile che coincide con la ragione sociale dell'azienda è seguita dalla stringa fissa "- Fatture scadute".

La catena d'infezione

Il file di script .vbs, una volta eseguito avvia la catena d'infezione copiando i due eseguibili di sistema powershell.exe e bitsadmin.exe dalle loro directory legittime (rispettivamente c:\Windows\SysWOW64\WindowsPowerShell\v1.0\ e c:\Windows\SysWOW64\) nella directory nascosta %programdata%

di Windows, rinominandoli successivamente con un nome casuale in modo da rendere più complessa un'eventuale ricostruzione della catena d'infezione.

Nel dettaglio, spiegano gli analisti del CSIRT, i due file binari copiati e rinominati vengono quindi utilizzati come segue:

- bitsadmin.exe per scaricare il file di secondo stadio e salvarlo nella cartella nascosta %appdata%;
- powershell.exe per eseguire il contenuto del file appena scaricato.

Come difendersi

Non è la prima volta che i criminal hacker diffondono sLoad tramite campagne di spam, inviando e-mail che contengono un allegato malevolo nella speranza che qualcuno lo apra, e molto probabilmente non sarà nemmeno l'ultima. Nella fattispecie le e-mail PEC includono, come visto, un file di archivio .zip che contiene al suo interno un file di scripting dannoso (.vbs, .vbe, .wsf, .wsc), ma i file che di solito vengono propinati come allegati malevoli possono essere anche documenti .doc, PDF, file eseguibili .exe o JavaScript.

I casi in esame rappresentano dei tentativi di truffa, che dimostrano ancora una volta come il problema, talvolta, non risieda nei sistemi di sicurezza (in questo caso delle PEC) quanto piuttosto nella scarsa gestione e conservazione delle credenziali da parte dei titolari (anch'essi vittime) le cui identità digitali violate vengono, successivamente, utilizzate in modo non autorizzato come mittenti in campagne di questo tipo.

Per tale motivo è altamente consigliato a tutti gli utenti e organizzazioni, per far fronte a questa tipologia di attacchi, di verificare scrupolosamente le e-mail che si ricevono eseguendo anche degli accorgimenti ulteriori di carattere

pratico:

- Non aprire allegati o link web presentati in e-mail (anche se PEC) irrilevanti o ricevute da indirizzi sconosciuti e sospetti;
- caricare file e programmi da fonti ufficiali, evitando downloader/installer di terze parti non affidabili;
- scansionare regolarmente i propri sistemi operativi alla ricerca di minacce con antivirus o antispyware affidabili e tenuti aggiornati;
- evitare di abilitare l'esecuzione delle macro nel caso di allegati Microsoft Office apparentemente legittimi;
- fornire periodiche sessioni di formazione finalizzate a riconoscere le possibili e-mail di phishing, alfine di assimilare questi concetti e prendere coscienza che gli atti criminosi possono concretizzarsi anche attraverso gli strumenti informatici.

Malware sLoad, in Italia nuova campagna malevola via PEC. L'allarme del CSIRT

'INAIL e la cultura cybersecurity: dal DevSecOps alla tutela del patrimonio applicativo'. Partecipa al webinar

Emerasoft e **Sonatype** presentano per la prima volta un evento digitale live per raccontare e condividere con il pubblico

come è possibile implementare al meglio la metodologia **DevSecOps** facendo della sicurezza parte integrante del processo di sviluppo e rilascio delle applicazioni.

Registrati

Ospite d'eccellenza è **Adele Gambacorta**, Responsabile Ufficio Supporto al processo di produzione e Certificazione, Direzione centrale per l'organizzazione digitale di **INAIL**.

L'evento ha l'obiettivo di condividere un vero e proprio progetto di trasformazione digitale che in INAIL è nato dall'esigenza di miglioramento del processo di release e *deploy* management, per poi evolversi in una vera e propria presa di coscienza del patrimonio *open source* detenuto in produzione e dei numerosi rischi a cui si è esposti. Un'occasione per conoscere da vicino una realtà come INAIL che in contrasto con le proprie dimensioni, conserva un'attitudine all'innovazione e una elevata cultura della sicurezza applicativa. Partecipa per scoprire quanto è importante avere una *Bill Of Material* delle tue applicazioni, e che un'analisi statica del codice non è sufficiente a metterti al riparo da attacchi malevoli.

PROGRAMMA

- **Tavola Rotonda virtuale a cui prenderanno parte:**
- **Adele Gambacorta**, *Responsabile Ufficio Supporto al processo di produzione e Certificazione, Direzione centrale per l'organizzazione digitale di INAIL*
- **Marco Pantano**, *DevSecOps consultant, responsabile del progetto DevSecOps di Inail*
- **Fabrizio Corsaro**, *Customer Success Engineer at Sonatype*
- Modera: **Riccardo Bernasconi,** *Sales Director di Emerasoft*
- Sessione Q&A.

Registrati

https://www.key4biz.it/inail-e-la-cultura-cybersecurity-dal-devsecops-alla-tutela-del-patrimonio-applicativo-partecipa-al-webinar/332466/

Report Enisa sulla cybersecurity nella mobilità

connessa e autonoma in Europa

L’ecosistema dei servizi e delle infrastrutture per la mobilità connessa e autonoma (***Connected and automated mobility***, Cam) si compone di innumerevoli soluzioni tecnologiche, frutto di investimenti e di un gran lavoro di sviluppo da parte di un’ampia e variegata platea di *stakeholders*, industrie e imprese.

Il **tema della *cybersecurity*** risulta quindi centrale dal momento che stiamo parlando di veicoli connessi in rete e fortemente caratterizzati dall’utilizzo di tecnologie software.

A chiedere più sicurezza informatica sono proprio i cittadini, i futuri passeggeri di questi mezzi connessi e a guida autonoma, che ovviamente esigono certamente mezzi confortevoli, ma anche affidabili, facilmente accessibili e sostenibili in termini ambientali.

Il Rapporto Enisa

Il **nuovo Rapporto** pubblicato dall’Agenzia europea per la cyber sicurezza (**Enisa**), dal titolo “***Cybersecurity stocktaking in the Cam***”, è centrato proprio sui principali pericoli informatici che potrebbero riguardare reti, servizi e software relativi all’ecosistema Cam.

Le minacce informatiche d’altronde sono numerose e sempre più insidiose in termini di sicurezza di mezzi, infrastrutture ed esseri umani, per questo motivo la platea di soggetti interessati è vasta: dalle associazioni di settore agli operatori automotive, dai fornitori di servizi ai Governi e le Autorità regolatorie nazionali, dalle imprese dei sistemi di

trasporto intelligente all'industria automobilistica, dagli fornitori di sistemi smart city ai fornitori di tecnologie software e hardware, fino agli operatori delle reti di telecomunicazione e ICT.

Cam e cybersecurity

Non meno importante ai fini dello sviluppo di questo nuovo tipo di mobilità pubblica e privata sono le disposizioni relative ai regolamenti di *cybersecurity* e agli upgrade software proposte dalle Nazioni Unite, adottate dal Forum Mondiale per l'Armonizzazione delle Normative sui Veicoli (WP.29), gruppo di lavoro della divisione Trasporti sostenibili della Commissione economica per l'Europa delle Nazioni Unite (UNECE), che ora devono essere recepite dalla Commissione europea e dagli Stati membri.

Si tratta di **un regolamento che dovrebbe entrate in vigore da luglio del 2022**, finalizzato ad imporre a tutti gli stakeholders e in primis alle case automobilistiche standard molto elevati di cybersecurity.

Un mercato in crescita

Un nuovo studio pubblicato da Markets and Markets ha stimato che **il mercato dei servizi e delle tecnologie cybersecurity per la mobilità connessa e autonoma potrebbe raggiungere i 4 miliardi di euro entro il 2025**.

Un settore questo dalla Cam, infine, che complessivamente a livello globale potrebbe arrivare a valere più di 556 miliardi di dollari entro il 2026, secondo uno studio Allied Market Research.

https://www.key4biz.it/report-enisa-sulla-cyber-sicurezza-della-mobilita-connessa-e-autonoma-in-europa/332330/

Cnr, Cini e Cnit: la creazione di un Istituto italiano di cybersicurezza è strategica per il Paese

"*Abbiamo appreso da notizie di stampa dell'interesse da parte del governo per la realizzazione del progetto, già previsto dal Piano nazionale cyber del 2017, per la creazione di un* ***Istituto Italiano di Cybersicurezza****, la cui necessità è stata evidenziata in tante occasioni dagli esperti del settore che lo considerano necessario per garantire la protezione del Sistema Paese sul piano cibernetico e indispensabile per il suo sviluppo economico*", ha dichiarato coralmente il **Comitato Nazionale per la Ricerca nella Cybersecurity**, di cui fanno parte: il Consiglio Nazionale per le Ricerche (**Cnr**), il Consorzio Interuniversitario Nazionale per l'Informatica (**Cini**) e il Consorzio Nazionale Interuniversitario per le Telecomunicazioni (**Cnit**).

I tre organismi di ricerca, da anni dedicati a sostenere il progresso della ricerca, dello sviluppo e della consapevolezza dei rischi nell'ambito della sicurezza informatica, sono tra i principali promotori in Italia di numerose attività in ambito accademico legate a tale tema.

"*Le sfide con le quali dobbiamo confrontarci quotidianamente sono sfaccettate e vanno dalle minacce informatiche verso le aziende fino a quelle contro le pubbliche amministrazioni*", è stato osservato nel documento.

"*Finora l'Italia ha dimostrato grande capacità di resilienza, e le sue aziende e università hanno lavorato rafforzando le competenze specifiche che tali nuove minacce richiedono. Tuttavia* – è specificato – *da anni chiediamo che i nostri sforzi vengano messi a sistema, a servizio del Paese, per una migliore protezione dei nostri asset fondamentali, che vanno dalle strutture sanitarie e ospedaliere (costantemente bersagliate da attacchi con finalità di profitto) fino al settore della ricerca, che specialmente in questo periodo potrebbe essere particolarmente esposto a campagne di spionaggio virtuale*".

"*La creazione di un Istituto Italiano di Cybersicurezza è ora più che mai strategica per amplificare e potenziare il lavoro dei singoli operatori della cyber security*", hanno aggiunto i membri del Comitato.

"*Da un lato l'imminente creazione dello European Cybersecurity Competence Center richiederà l'attivazione di una rete di analoghi centri nazionali, e l'Italia ne è ancora purtroppo sprovvista. Dall'altra* – è precisato – *la pandemia ha già provato duramente il sistema socio-economico del Paese, ed è quindi ancora più importante che in un momento come questo il Governo si impegni a rafforzare le infrastrutture e gli strumenti che abilitano la trasformazione digitale del Paese, per favorire quindi la ripresa economica: la sicurezza informatica è tra queste*".

"*In quest'ottica* – si legge nella dichiarazione – *un Istituto Italiano di Cybersicurezza, caratterizzato da una struttura centralizzata, multidisciplinare e con adeguata massa critica, che permetta una collaborazione efficiente ed efficace delle istituzioni con il mondo della ricerca pubblica e privata è indispensabile per lo sviluppo di piattaforme e di adeguate soluzioni architetturali al servizio del Paese e della sua ripartenza*".

L'executive board del *Comitato Nazionale per la Ricerca in*

Cybersecurity:
Marco Conti e **Fabio Martinelli** (Cnr)
Rocco De Nicola e **Paolo Prinetto** (Cini)
Nicola Blefari Melazzi (Cnit)

Per saperne di più: CNR
Cnr, Cini e Cnit: la creazione di un Istituto italiano di cybersicurezza è strategica per il Paese

---

Partecipa all'evento digitale 'Inail e la gestione delle librerie Open Source nel percorso DevSecOps'

Emerasoft e **Sonatype** presentano per la prima volta un evento digitale live per raccontare e condividere con il pubblico come è possibile implementare al meglio la metodologia **DevSecOps** facendo della sicurezza parte integrante del processo di sviluppo e rilascio delle applicazioni.

Ospite d'eccellenza, per raccontare il caso d'uso **Inail**, è **Adele Gambacorta**, Responsabile Ufficio Supporto al processo di produzione e Certificazione, Direzione centrale per l'organizzazione digitale.

L'evento ha l'obiettivo di condividere un vero e proprio progetto di trasformazione digitale che in Inail è nato dall'esigenza di miglioramento del processo di release e *deploy* management, per poi evolversi in una vera e propria presa di coscienza del patrimonio *open source* detenuto in

produzione e dei numerosi rischi a cui si è esposti. Un’occasione per conoscere da vicino una realtà come Inail che in contrasto con le proprie dimensioni, conserva un’attitudine all’innovazione e una elevata cultura della sicurezza applicativa. Partecipa per scoprire quanto è importante avere una *Bill Of Material* delle tue applicazioni, e che un’analisi statica del codice non è sufficiente a metterti al riparo da attacchi malevoli.

PROGRAMMA

- **Tavola Rotonda online a cui prenderanno parte:**
- **Adele Gambacorta**, *Responsabile Ufficio Supporto al processo di produzione e Certificazione, Direzione centrale per l’organizzazione digitale*
- **Marco Pantano**, *DevSecOps consultant, responsabile del progetto DevSecOps di Inail*
- **Fabrizio Corsaro**, *Customer Success Engineer at Sonatype*
- Modera: **Riccardo Bernasconi,** *Sales Director di Emerasoft*
- Sessione Q&A.

Registrati

Partecipa all’evento digitale ‘Inail e la gestione delle librerie Open Source nel percorso DevSecOps’