5 Simple Yet Effective Ways to Increase Data Security



According to the Better Business Bureau, U.S. small businesses lost an average $79,841 from cyberattacks in 2017. What are you doing about this in 2019?

January 7, 2019 5 min read

Opinions expressed by *Entrepreneur* contributors are their own.

Business data is more than propriety information. Most small businesses hold customer credit card information on file and maintain electronic employee records, as well as manage their banking online. And a breach of this data disrupts basic operations and damages your reputation not to mention probably costing you thousands of dollars.

Related: Here's How You Can Secure Your Data with Blockchain

Symantec, in fact, recently released a study describing how cyberattacks against small businesses are on the rise and are expected to increase in the coming years. With the Better Business Bureau reporting that U.S. small businesses lost an average $79,841 from cyberattacks in 2017, it makes sense to take action to avoid these potential losses. Here's how:

Conduct a cybersecurity audit.

The best way to defend against a cyberattack is to understand the areas of vulnerability and develop an action plan to address them. The Financial Industry Regulatory Authority (FINRA) has created a Small Firm Cybersecurity Checklist that is free to download and is basically an audit tool that helps you identify areas where your data is vulnerable to outside exploitation.

The checklist also points out other needs, such as employee-data management training, incident-response systems and other actions you can take to better secure your data. The checklist includes areas where you should document the remediation steps necessary to better secure your information.

Once completed, the checklist will show you exactly where you currently stand with regard to data security as well as provide a detailed action plan for improvement.

Train and monitor your employees.

Employee training of secure data management is important, but so is teaching your team to identify and report potential internal breaches. The IBM 2016 *Cyber Security Intelligence Index* found that 60 percent of all cyberattacks were carried out by people inside the companies surveyed. Of those insider attacks, three-quarters were carried out with malicious intent and the other quarter were committed by inadvertent actors.

Related: How Social Media Jeopardizes Data Security

For small businesses, protecting yourself from this type of internal threat begins with your onboarding process. Train employees on cybersecurity measures within the company and review the penalties, both internal and criminal, for intentional breaches. When an employee leaves, either voluntarily or not, conduct an out-boarding interview that reviews these penalties and then change all passwords and other security codes that the person used to assure that he or she cannot gain physical or electronic access to your business operations after leaving.

Manage information access.

Since most cyberattacks occur from internal sources, another way to protect your data is to limit access. Not every employee needs access to every account, database or file. Review all employees' roles within the company and give them access only to that information they need to perform their job. According to CompuQuip, you should classify your data and set up controls or tools to manage access.

This process protects your data in two ways. First, it limits how much information each employee can access, which will narrow the amount of harm that can occur if it is used for non-business purposes. Second, it will limit the damage that can occur if the employee is the victim of a phishing attack or other malware infection, since not all data systems will be accessed.

Set up automatic software updates.

Cybercriminals analyze software programs for vulnerabilities and exploit those weaknesses whenever possible. The newer the software version you are running, the more protected it is from attacks. According to Comodo Antivirus, updating your

antivirus, operating system, and other software regularly lessens your risk of being infected by malware or becoming the victim of ransomware attacks.

Few businesses take the time to update their systems on a regular basis, but most software packages offer the option of automatic updates. Utilizing this feature is one of the best protections you have against external threats.

Use a decentralized virtual network.

You may think you're secure, but many business messenger and communication systems may be collecting your business data and communication history. This information may be used for the host's own use or harvested by other companies without your knowledge or permission. For example, Facebook was recently fined £500,000 by the U.K.'s Information Commissioner's Office for the social media platform's part in the Cambridge Analytica scandal. The reality is that delegating your data and privacy to an outside system leaves you vulnerable to this type of misuse of your information.

For this reason, Zangi Messenger's experts recommend creating your own secure and independent communication network for full control over your business data. This decentralized vertical network is hosted on your own company servers or clouds, giving you complete control over who has access to your information and how it is used.

Document-sharing, messaging and other standard business activities can then occur anywhere without risk of data breaches or malware downloads, making this a great solution for small companies conducting a lot of business away from the office.

Related: Importance of Data Security in the Age of Artificial

Intelligence

Bottom line

Cybersecurity is a necessity that too many small businesses put on the back burner, but this lapse can lead to severe financial losses. Instead, conduct an internal audit, train and monitor employees and update your software regularly to better protect yourself. If you conduct most of your business out of the office, utilize a decentralized virtual network to keep your data secure wherever you go.

https://www.entrepreneur.com/article/325813

How Secure Is Your Messaging App?



Here’s how to tell whether your private messages could be hijacked or whether they’re safe from prying eyes.

December 27, 2018 7 min read

This story originally appeared on PC Mag

Which messaging app would you choose for absolute security? Every developer will profess that they responsibly consider the security and privacy of their users. But with so many different choices, it can be hard to tell which messaging platforms you can trust.

This set of criteria can help you evaluate the security of your messaging apps and decide how far you can trust them.

Encryption

Virtually no messaging app sends your messages in clear text format; all platforms use some form of encryption to scramble messages and prevent unauthorized parties from reading them.

But not all forms of encryption are equally secure.

Some apps encrypt your messages in transition and storage, but also hold a copy of the encryption keys. This means they can decrypt and read the content of your messages. Companies that use this form of encryption usually do so to mine user data for advertising purposes. Examples include the soon-to-be-phased-out Google Hangouts, Skype, and WeChat.

Related: Security Trends Your Company Needs to Embrace in 2019

But if the servers of these companies fall victim to a data breach, malicious actors will gain access to the keys and can also decrypt your messages. The companies that host these services are then open to warrants from government agencies that want to investigate users' private communications.

The most secure platforms employ end-to-end encryption (E2EE). These apps use public key cryptography to encrypt messages: For each user, the platform issues a pair of public and private encryption keys. It stores the public keys on its servers, but private keys are stored on user devices only.

Users can retrieve one another's public keys from the servers to encrypt their messages. Each message encrypted with a public key can only be decrypted with its corresponding private key, which is in the exclusive ownership of the recipient. End-to-end encryption ensures that not even the company that hosts the application can access a message's content. Even if hackers break into their servers or three-letter agencies force them to hand over user data, they won't be able to decrypt the content of messages.

At present, more and more platforms are adopting end-to-end encryption. Some examples include Signal, WhatsApp, Wickr, and Apple's iMessage.

Other messaging apps such as Telegram and Facebook Messenger also support end-to-end encryption, but it's not

turned on by default. You have to enable the feature manually for individual chats. Skype also recently added a feature called Private Conversation that provides end-to-end encrypted chat, but it also is not the default configuration.

Message Deletion

Although end-to-end encryption protects you against eavesdroppers, it’s of no use if your device or the devices of the people you chat with fall into the wrong hands. Another security feature to look for in messaging apps is the ability to remove messages after they’re sent. Deleting messages ensures that if one of the devices becomes compromised, your sensitive communications aren’t exposed.

Related: What’s Happening on The Entrepreneur Index Right Now

Telegram, Signal, and Skype let users delete messages for themselves and the recipients of their messages. Wickr also has a “recall message” feature, which deletes messages from the devices of everyone involved in a conversation. And WhatsApp added a “delete for everyone” option last December, but you can use it to delete only those messages you’ve sent within the last 13 hours.

iMessage doesn’t support the deletion of individual messages: You can delete only entire chats, and when you do so, you’re removing a chat only from the device you’re using; it stays on all other iOS devices that share the same Apple ID as well as on the devices of the person you were chatting with.

A convenient addition to deletion is the self-deleting message. This feature will automatically remove messages from the devices of all users after a certain amount of time expires. On Signal, it’s called “disappearing messages.” When you turn on the feature, you specify an expiration time after which a message is automatically removed from all devices.

Wickr's self-destruct feature is called "Burn-on-read." Telegram and Facebook Messenger also support self-destructing messages but only for their secret chat features that run on end-to-end encryption. WhatsApp doesn't support self-deleting messages.

Note that if the receiver of a message takes a screenshot of your chat and stores it elsewhere, deletion will be pointless; message deletion won't protect you against malicious conversation partners. Rather it's a safeguard against unintentional mistakes.

Metadata

Along with the content of messages, you should be concerned about metadata—the information that a messaging platform stores about your activities. Metadata includes sender and receiver IDs, the time a message is sent, login times, IP addresses, device types, duration of calls, and other information that can reveal your identity and habits.

Related: The Dangers of the Internet of Things (Infographic)

In the wrong hands, metadata can be very harmful, because it can reveal a user's communication patterns: the people they're in contact with, their geographical location, the timing of their messages, and more.

Most popular messaging applications collect a wealth of information about user activity. But Signal has the best track record, since it registers only the phone number with which you created your account and the last date you logged in to your account (not including the hour, minute, and second).

Transparency

Beyond the promises of developers, independent experts should be able to verify the security of a messaging application.

Open-source platforms — applications whose developers make the source code available publicly — are generally more reliable, because they usually undergo thorough peer review and cross-examination by other developers and security experts.

Signal is open-source, and the source code of all versions of the app is available for download on GitHub. Wickr made its source code publicly available last year. Telegram also provides the source code of its apps and lets developers create and publish their own versions of the client app that can hook into its application programming interface (API).

Related: Google Home and Amazon Echo Can Store Your Voice Recordings. Here's When They Could Be Used Against You.

WhatsApp and Facebook Messenger are not open-source, but they do use the open-source Signal Protocol to encrypt users' messages.

Closed-source apps such as iMessage require users to fully trust the developer to check its code for security bugs and not to install backdoors: intentional vulnerabilities meant to provide select parties (say, advertisers and government agencies) access to encrypted message content.

Nothing's Perfect

To sum up, when you're evaluating a messaging app, ask yourself these questions:

- Does it use end-to-end encryption?
- Does it allow message deletion for all parties to a conversation?
- How much metadata does it collect?
- Is the source code open for review, and have outside experts confirmed its security?

Answering them will give you a good sense of how secure a messaging app is.

But to be clear, there’s no such thing as absolute security. And even the most secure messaging platform won’t protect you against yourself.

In addition to choosing a secure messaging app for your sensitive communications, you should develop personal safety habits such as setting a screen lock on your devices, not installing apps from unknown developers, and not oversharing online. The best way to have a private conversation is to avoid online platforms altogether.

https://www.entrepreneur.com/article/325395

Security Trends Your Company Needs to Embrace in 2019

IT innovations create risk until new cyber security solutions, like AI and authentication, rise up to meet the challenges they present. https://www.entrepreneur.com/article/321539

The Sneaky Way SEO Spam Is Costing You Business — And

How to Stop It

Is your website at risk? https://www.entrepreneur.com/article/322639

Looking to Change Jobs? This Industry Has 0 Percent Unemployment. (Infographic)

There’s a talent gap in cybersecurity. https://www.entrepreneur.com/article/321657

La California ‘banna’ le password facili (admin, 12345) per contrastare gli hacker

Gli studi sulla sicurezza informatica hanno dimostrato come una combinazione tra password deboli e software non aggiornati possono consentire ai cybercriminali di prendere completo controllo di account, router e informazioni personali all’interno dei propri laptop. Per questo motivo lo Stato americano della **California** l0 scorso 29 settembre ha approvato la nuova legge sulla Privacy chiamata: ‘The Information

Privacy: Connected Devices bill (SB-327)‘.

La legge

La legge sulla privacy delle informazioni: **Connected Devices** (SB-327) renderà illegale per le aziende che fabbricano un dispositivo connesso a Internet, come un router o una webcam, impostare una password predefinita debole sul dispositivo. In questo momento molti router sono stati dotati della password amministrativa “admin” o “password”, che gli utenti sono quindi tenuti a modificare in qualcosa di più complesso dopo averlo configurato nella loro casa. Naturalmente, la maggior parte degli utenti raramente lo fa, il che significa che gli hacker hanno un tempo molto facile per accedere ai loro dispositivi collegati in rete.

A partire dal 2020, sarà illegale per i produttori di dispositivi connessi a Internet impostare tali semplici password predefinite su tali dispositivi. Il disegno di legge richiederà ai produttori di impostare password di amministratore complesse e univoche sui propri dispositivi o una procedura di avvio che richieda all’utente di creare una password complessa durante la configurazione del dispositivo per la prima volta.

Come sottolinea la BBC, le semplici password di amministratore per i dispositivi connessi a Internet hanno portato gli hacker a essere in grado di utilizzare offline siti come Twitter, Spotify e Reddit. La nuova legge entrerà in vigore in California il 1 ° gennaio 2020.

Il 2017 l’annus horribilus della cybersecurity

Il 2017 è stato l’annus horribilis della sicurezza informatica, travolto dalla diffusione dei ransonware WannaCry e NotPeya, dall’esplosione del phishing e dalle truffe online.

La causa principale delle falle nel settore cybersecurity resta il fattore umano, come evidenziato nell’ultimo report di **Proofpoint “Human Factor 2018**″, dove gli hacker lavorano sempre più per cercare di sfruttare le persone e le loro debolezze per il furto di denaro e dati. Debolezze appunto, perché le persone sono la vera causa dei principali attacchi informatici.

Le password sono i custodi fondamentali delle nostre identità digitali, permettendoci di accedere ad acquisti online, appuntamenti, attività bancarie, ai social media e alle comunicazioni personali.

Molte persone usano password semplici, come; ‘1234567’, ‘qwerty’ e anche ‘password.’ (Vedi le peggiori password del 2017). Tuttavia, usando programmi di cracking delle password, gli hacker possono violare queste molto facilmente. Questi programmi fanno supposizioni multiple ad alta velocità fino a quando la password non è completamente decifrata. Il programma potrebbe richiedere alcuni minuti o anni; tutto dipende dalla complessità della password. Se la password è semplice, può essere violata in pochi secondi.

The post La California ‘banna’ le password facili (admin, 12345) per contrastare gli hacker appeared first on Key4biz.

https://www.key4biz.it/la-california-banna-le-password-facili-admin-12345-per-contrastare-gli-hacker/233939/

Quantum computing, l’evoluzione da bit a qubit

La sicurezza e gli algoritmi usati per crittografia e la lunghezza di password sono basati sull’attuale tecnologia Hardware che abbiamo a disposizione. Mettere una chiave lunga e complessa per entrare nel nostro sistema operativo o sui siti è considerato abbastanza sicuro poiché un attaccante avrebbe bisogno di molto tempo con l’attuale potenza di calcolo disponibile per decrittografare la password e vedere le informazioni. Per crittografia si intente, come ricorda **Wikipedia**, la branca che tratta le “scritture nascoste”, i metodi per rendere un messaggio “offuscato”, in modo da non essere comprensibile a persone non autorizzate a leggerlo.

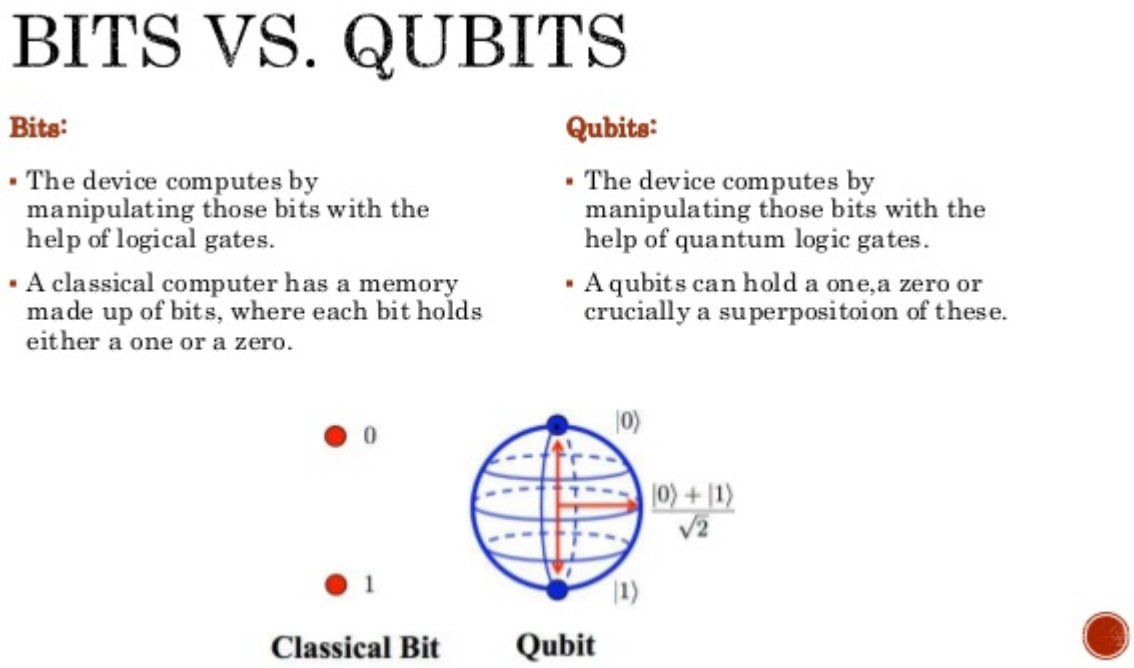
La regola considerata come modus-operandi che tutti i consulenti di sicurezza informatica al momento usano è incentivare/obbligare l’utente a inserire caratteri particolari, maiuscole, minuscole e numeri per aumentare la complessità che la password non venga scoperta. Un esempio potrebbe essere una password su crittografia simmetrica da 2 caratteri, per scoprirla il Pc deve fare tutte le combinazioni finché non trova la giusta password, ma all’aumentare dei caratteri, esempio 10, le interazioni e combinazioni aumentano elevando così anche il tempo per trovare una chiave. Un computer per trovare password lunghissime comincia a impiegare mesi, anni,..ecc. I recenti sistemi con schede video in parallelo che sfruttano il sistema **Nivida-CUDA**, per decrittografare informazioni crittografate, hanno aumentato di molto la potenza di calcolo. Potenza usata sia per simulazioni da parte di ricercatori ma anche per scoprire dati

crittografati raccolti da un potenziale cracker.

I computer che ci circondano ai giorni d'oggi usano i Binary Digit (bit), i due segnali che permettono di memorizzare i dati 0-1 un byte raccoglie 8 bit. Nella storia dei pc i bit hanno assunto diversi ruoli come nei transistor aperto-chiuso o porzioni di disco fisso meccanico, materiale magnetizzato in un verso o nell'altro. Il codice binario è alla base di tutti i computer. I bit vengono raggruppati in 32-64 bit per memorizzare porzioni più grandi di informazioni massime che il computer riesce a gestire. I computer possono volgere attraverso le porte logiche lavori della logica booleana come not, and, or, nand, xnor, nor e xor. I computer quantistici usano i qubit invece di bit, mentre sui pc attuali gli stati sono spento o acceso quindi 1 o 0 nei qubit possiamo avere una sovrapposizione coerente di stati. Questa sovrapposizione indica che è sia in uno stato sia nell'altro rispetto alla logica che conosciamo binaria. Questo stato permette al computer quantistico di avere molta più potenza di calcolo rispetto al sistema classico. Le porte logiche sono 9 nei Pc quantistici. Queste condizioni sono alla base della potenza di calcolo nella *Quantum computing*. L'algoritmo è una sequenza di azioni per ottenere un risultato, Wikipedia suggerisce, procedimento che risolve un determinato problema attraverso un numero finito di passi elementari, chiari e non ambigui, in tempo ragionevole. Nella struttura di un computer classico, anche se avesse molte Cpu in parallelo, molta Ram e frequenza di clock alta, la workstation dovrebbe usare un algoritmo che dato un input, seguendo delle regole per decrittografare, otterrebbe un risultato valido in tempi ragionevoli calcolati nella vita di un uomo. Ogni problema viene risolto con un algoritmo adatto per avere il risultato nel modo più veloce.

Nella sicurezza informatica per scoprire le password viene

usato il metodo brute-force o dizionario. Mentre nella prima il tempo è elevato perché va a provare tutte le combinazioni, mentre il secondo, dato un dizionario pronto prova meno interazioni per trovare la chiave, se contenuta nel dizionario.



Gli algoritmi si suddividono in efficienti e non efficienti. I primi se la sua complessità è di ordine polinomiale, esempio 2xN, o una qualche potenza mentre i secondi se la sua complessità è di ordine superpolinomiale ovvero 2 alla N. I computer quantistici sfruttano algoritmi quantistici diversi dai classici ovvero cercare più soluzioni contemporaneamente sfruttando la sovrapposizione di stati. I più famosi sono due algoritmi di **Grover** e di **Shor**. Se dovessimo trovare una password dentro a un file contenente 1000 parole quindi mille prove, il pc classico dovrebbe fare tutte le prove mentre il pc quantistico con l'algoritmo di Grover impiegherebbe la radice quadrata del numero da esaminare. L'algoritmo di **Peter Shor** lavora invece la fattorizzazione di numeri con più di 100

cifre. Se per trovare una password o decrittografare una sessione *sniffata* di un traffico dati di qualche comunicazione con i Pc tradizionali, che usano algoritmi classici si impiegherebbe un certo tempo mentre con i Pc quantistici molto meno della metà. Complessi calcoli necessitano di molto tempo di elaborazione che codificano i due stati descritti, i computer quantistici sono in via di sviluppo e non vi è ancora uno standard definito. Aziende, come **IBM**, **Google**, **Intel**, e università come MIT e Harvard stanno sviluppando computer quantistici, questo porta a dover nel futuro prossimo, partendo già da ora, rivisitare la nostra sicurezza, nel modo di concepire la security IT e nel modo di proteggere le nostre comunicazioni.

The post Quantum computing, l'evoluzione da bit a qubit appeared first on Key4biz.

https://www.key4biz.it/quantum-computing-levoluzione-da-bit-a-qubit/233878/

Cyber-spionaggio con microchip, perché la Cina spia Amazon e Apple

Chip grandi quanto una punta di matita inseriti nei server di 30 aziende americane hi-tech (di cui spiccano **Amazon** e **Apple**) posizionati in maniera da tale da non essere visti e scoperti da nessuno e con l'obiettivo di raccogliere più informazioni possibili.

Lo scoop della rivista settimanale Businessweek dell'agenzia Bloomberg ha fatto il giro del mondo in poche ore. Un'indiscrezione pesante che, seppur smentita dalle aziende interessate, ha avuto un impatto dirompente sulle Borse asiatiche e in particolar modo sui titoli delle società produttrici del comparto tecnologico, affossando i produttori tech.

> *NEW COVER: The Big Hack*
>
> *China used a tiny chip in a huge hack that infiltrated Apple and Amazon https://t.co/GVLBnWaaue pic.twitter.com/4aNdEwPzAF*
>
> *— Businessweek (@BW) 4 ottobre 2018*

Il caso

Secondo l'inchiesta condotta da Bloomberg, l'unità militare cinese – **People's Liberation Army-** ha inserito dei minuscoli microchip nei server dei computer utilizzati da aziende come Apple e Amazon che forniscono alla Cina un accesso backdoor a computer e dati. I chip, piccoli come la punta di una matita affilata e progettati per essere non rilevabili senza attrezzature speciali, sono stati impiantati sulle schede madri dei server sulla linea di produzione in Cina.

La responsabilità della sua installazione nell'hardware è stata attribuita al termine di un'indagine ad alcuni membri di un'unità dell'Esercito Popolare di Liberazione, le forze armate della **Repubblica Popolare Cinese,** presenti nelle fabbriche di **Super Micro Computer**. L'azienda progetta le sue apparecchiature a **San Jose** in **California**, ma, come la maggior parte delle aziende di elettronica, esternalizza la

produzione, compresi gli appaltatori in Cina.

Sempre secondo l'inchiesta, l'attacco è stato scoperto nel 2015 dai servizi di intelligence statunitensi, nonché da Apple e Amazon mentre le società acquistavano server realizzati da Super Micro Computer. Il rapporto afferma che Amazon è venuta a conoscenza dell'attacco durante le mosse dalla sua controllata **Amazon Web Services** (AWS) per acquistare la società di compressione video streaming **Elemental Technologies** nel 2015.

Apple avrebbe acquistato circa 7000 server Super Micro quando i suoi team di sicurezza hanno scoperto i chip. Secondo il rapporto citava 17 fonti di intelligence e fonti anonime che affermavano che le spie cinesi avevano collocato chip informatici all'interno di apparecchiature usate da circa 30 società, oltre a più agenzie governative statunitensi, il che avrebbe garantito a **Pechino** l'accesso segreto alle reti interne.

Tutti negano

Amazon, Apple e Super Micro hanno completamente negato l'inchiesta di Bloomberg. Amazon ha dichiarato: "*Non è vero che AWS fosse a conoscenza di un compromesso nella catena di fornitura, di un problema con chip dannosi o di modifiche all'hardware durante l'acquisizione di Elemental.*" AWS ha dichiarato: *"Come abbiamo condiviso con Bloomberg BusinessWeek più volte negli ultimi due mesi, in nessun momento, passato o presente, abbiamo mai riscontrato problemi relativi all'hardware modificato o ai chip maligni nelle schede madri SuperMicro in qualsiasi sistema Elemental o Amazon.*" Apple ha affermato: "*Su questo possiamo essere molto chiari: Apple non*

ha mai trovato chip dannosi, manipolazioni hardware o vulnerabilità appositamente posizionate in alcun server”. “*Rimaniamo all’oscuro di tali indagini*“, ha dichiarato Super Micro.

Cyber-spionaggio

L’obiettivo ultimo dell’operazione, stando a quanto afferma un ufficiale USA, è per la Cina quello di avere accesso sul lungo periodo a segreti industriali e reti governative statunitensi. L’introduzione di chip spia nella catena di approvvigionamento sarebbe un’impresa significativa di cyber-spionaggio. Le rivelazioni di **Edward Snowden**, informatore della **NSA**, hanno mostrato che l’intelligence degli Stati Uniti ad esempio, preferisce introdurre di nascosto questi hardware negli articoli destinati al mercato cinese. Ma il problema resta sempre lo stesso: la Cina produce molto più hardware di quanto non facciano gli Stati Uniti.

Secondo il rapporto di Bloomberg, nel 2014 l’intelligence ha specificamente avvertito la **Casa Bianca** che le forze armate cinesi stavano pianificando di installare i chip sulle schede madri Supermicro. Ma poiché l’hardware di Supermicro è così ampiamente utilizzato, e l’obiettivo non è chiaro, e questa era un’importante azienda americana, a differenza di Huawei e ZTE, che sono state pubblicamente accusate di presentare minacce alla sicurezza – l’FBI ha fatto un passo indietro dall’emissione di un avviso pubblico. Quella reticenza continuò dall’amministrazione Obama all’amministrazione Trump.

Secondo **Kurt Baumgartner,** Principal Security Researcher di Kaspersky Lab: *“L’incidente riportato dai media sottolinea quanto possa essere furtivo un attacco fatto grazie a chip*

minuscoli, elaborati e accuratamente nascosti. Questi chip potrebbero potenzialmente alterare il sistema operativo o portare ad una diminuzione della sicurezza in generale, indebolendo, ad esempio, gli schemi di crittografia o aumentando i privilegi e le possibilità di accesso. C'è molto in gioco: comunicazioni personali e aziendali, traffico IP, dati dei clienti e molto altro ancora. Tuttavia, presto o tardi, il chip si metterà in comunicazione con i suoi proprietari ed è proprio nel momento in cui si metterà in contatto con il sistema di comando e di controllo degli attaccanti che la minaccia, prima sconosciuta, diventerà più vulnerabile.

E allora perché lo spionaggio? Ad oggi Super Micro è il principale fornitore di schede madri al mondo e detiene un monopolio nel business dei computer destinati ad ambiti specifici come le apparecchiature **MRI** per le analisi cliniche o i sistemi che gestiscono le armi. Tutto questo senza dimenticare istituti bancari, data center per il cloud, hosting per i servizi Web e molto altro ancora. Il suo business è ben rappresentato dalla descrizione fornita da un ufficiale dell'intelligence USA.

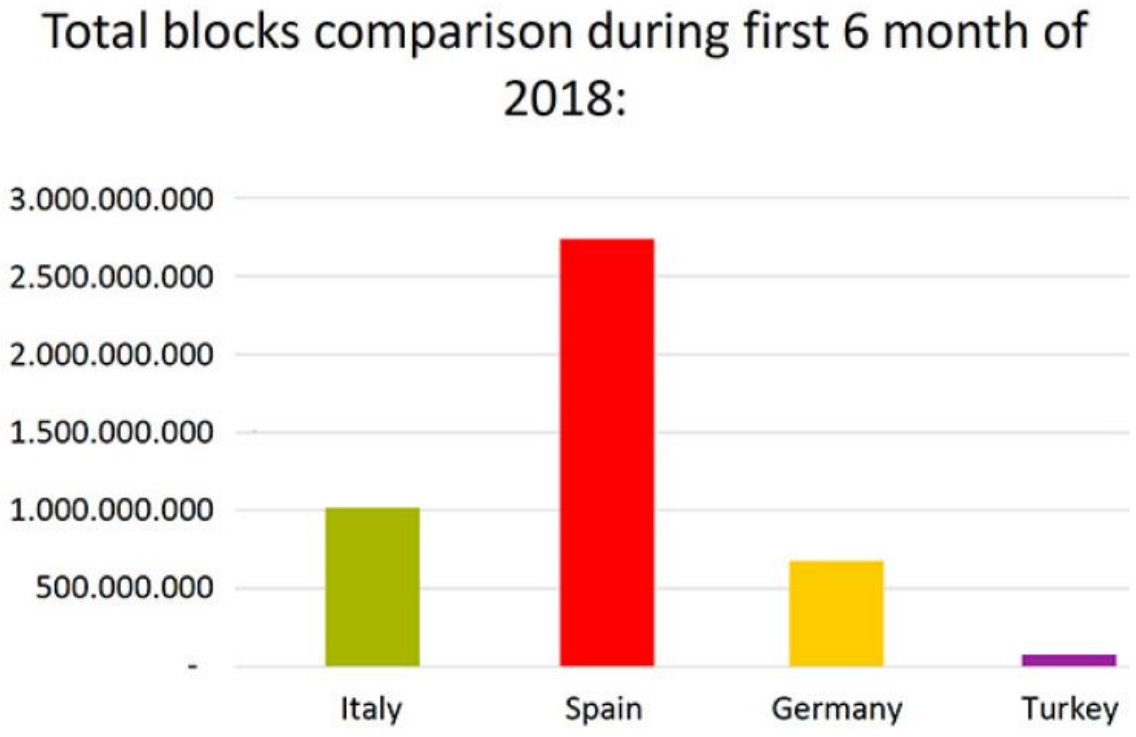
The post Cyber-spionaggio con microchip, perché la Cina spia Amazon e Apple appeared first on Key4biz.

https://www.key4biz.it/cyber-spionaggio-con-microchip-perche-la-cina-spia-amazon-e-apple/233832/

Vodafone, più che raddoppiati in un anno virus e malware bloccati da Rete Sicura

Più che raddoppiate in un anno le minacce informatiche bloccate da Rete Sicura, il servizio anti virus e anti malware di **Vodafone** che, grazie alla funzione *"Navigazione Protetta"*, consente ai clienti di navigare in maniera sicura sul web, sia da mobile, sia da rete fissa, evitando possibili attacchi virus e azioni di phishing.

Lo rende noto l'operatore, che in occasione del mese della cybersecurity ha pubblicato il primo report annuale su come i clienti Vodafone vengano protetti da virus e malware durante la navigazione su Internet grazie, appunto, a **Rete sicura**, il prodotto presente gratis in ogni offerta per i primi 2 mesi, che poi si rinnova a 1 euro al mese. Il servizio è gratuito con l'offerta Shake Remix Unlimited Junior.



Fra i principali dati che emergono dal **Vodafone Italy Secure**

Net Marketing Report relativi alla parte mobile, tra gennaio e giugno 2018 Rete sicura ha bloccato **935** milioni di minacce; si registra un incremento del **183% di virus** bloccati e **del 124.4% di malware**; la maggior parte delle minacce bloccate in questo periodo sono dovute al fenomeno di **criptomining** in Europa, generato da Coinhive.com. Nel report si riportano le maggiori minacce rilevate sul mese di agosto.

Come funziona Rete sicura? Si basa su una tecnologia direttamente integrata nell'infrastruttura di rete e non ha bisogno di app per funzionare. Grazie alla soluzione Allot, Rete Sicura integra due delle maggiori basi dati virus quali Kaspersky e Sophos. La tecnologia alla base è quella del "traffic inspection", che consente di analizzare sia la destinazione (URL o indirizzo IP) che il contenuto (i pacchetti dati) e, se infetti, di bloccarli alla fonte, tramite l'applicazione di filtri Antivirus e Parental Control.

Di seguito il report completo: https://www.vodafone.it/portal/Privati/Vantaggi-Vodafone/La-nostra-Rete-Veloce/Rete-Sicura/Vodafone-Rete-Sicura

The post Vodafone, più che raddoppiati in un anno virus e malware bloccati da Rete Sicura appeared first on Key4biz.

https://www.key4biz.it/vodafone-piu-che-raddoppiati-in-un-anno-virus-e-malware-bloccati-da-rete-sicura/233833/

Cybercrime, accordo tra Polizia di Stato e Wind Tre per la tutela delle reti

E’ stato siglato ieri a Roma l’accordo tra la **Polizia di Stato** e **Wind Tre S.p.A**. per la tutela delle reti e dei sistemi informativi dell’azienda, di particolare rilievo per il Paese.

La convenzione, firmata dal Capo della Polizia – Direttore Generale della Pubblica Sicurezza **Franco Gabrielli** e da **Jeffrey Hedberg,** Amministratore Delegato di Wind Tre S.p.A., è finalizzata a sviluppare una collaborazione strutturata tra la Polizia di Stato e le attività di Wind Tre S.p.A. per l’adozione di strategie sempre più efficaci in materia di prevenzione e contrasto al cybercrime.

Le piattaforme tecnologiche ed i sistemi di rete di Wind Tre S.p.A. costituiscono un asset fondamentale a tutela dell’interesse nazionale, grazie alle prestazioni fornite nell’ambito dei servizi di pubblica utilità.

Wind Tre S.p.A., infatti, considera la cybersercurity una priorità da tutelare insieme alla Polizia di Stato, attraverso interventi integrati che vanno dalla condivisione delle informazioni alla gestione congiunta dei piani operativi con i principali attori della sicurezza cibernetica.

Per la Polizia di Stato il supporto verrà assicurato dal **Centro Nazionale Anticrimine Informatico per la Protezione**

delle Infrastrutture Critiche (CNAIPIC) del Servizio Polizia Postale e delle Comunicazioni che, da anni, si occupa della tutela delle reti informatiche di realtà, sia pubbliche che private, di importanza strategica per il Paese.

Analisi dei rischi, scambio informativo, rapporti previsionali sull'evoluzione del cybercrime e sulle sempre crescenti minacce informatiche, gestione di eventi e situazioni critiche con il supporto della sala operativa attiva h24: queste sono alcune delle iniziative di collaborazione previste dall'accordo e che rappresentano un efficace strumento di difesa di fronte alla continua evoluzione delle minacce informatiche.

Alla firma della convenzione erano, inoltre, presenti per il Dipartimento della Pubblica Sicurezza, il Direttore Centrale per la Polizia Stradale, Ferroviaria, delle Comunicazioni e per i Reparti Speciali della Polizia di Stato, **Roberto Sgalla,** e il Direttore del Servizio Polizia Postale e delle Comunicazioni, **Nunzia Ciardi,** mentre per Wind Tre S.p.A., l'Amministratore Delegato, **Jeffrey Hedberg,** il Direttore PR Internal & External Communication, **Massimo Angelini** e il Direttore Litigation, Security & Lawful Data Services, **Vincenzo Folino.**

The post Cybercrime, accordo tra Polizia di Stato e Wind Tre per la tutela delle reti appeared first on Key4biz.

https://www.key4biz.it/cybercrime-accordo-tra-polizia-di-stato-e-wind-tre-per-la-tutela-delle-reti/233673/