Cybersecurity, Tofalo (Difesa): 'Presto defiscalizzazioni per le PMI'

"*La sicurezza informatica è in cima all'agenda del Governo la cui azione combinata punta a investire sullo sviluppo delle nuove tecnologie e la sensibilizzazione degli utenti attraverso la diffusione della cultura della sicurezza e la formazione*". Lo ha detto il sottosegretario alla Difesa **Angelo Tofalo** intervenuto ieri al convegno '*Cyber Security, un problema non solo tecnico*" organizzato a Milano con la **Regione Lombardia** e l'Associazione 'Tra il Dire e il Fare'.

"*La sicurezza* – ha aggiunto il sottosegretario – *è un bene comune, deve essere quindi considerata un investimento per la nostra comunità e non un costo, nell'ottica di Sistema Paese. Per questa ragione stiamo lavorando a una proposta per la defiscalizzazione dei costi per la sicurezza per le grandi ma soprattutto piccole e medie imprese*".

Per **Tofalo** quello di Milano "*e' stato un appuntamento che ha richiamato l'attenzione sui rischi e sulle opportunità del dominio cibernetico e su cosa fare per non incorrere nei pericoli della rete. Un tema che riguarda tutti, a ogni livello, dal singolo alle società e alle amministrazioni pubbliche*"

Esperti cyber cercasi

Nel frattempo l'Italia è alla ricerca di risorse interessate a far parte del personale del Comparto Intelligence e che intendono dare un concreto contributo alla missione del **DIS**, dell'**AISE** e dell'**AISI** a tutela degli interessi strategici nazionali in campo politico, militare, economico, scientifico e industriale.

La ricerca è rivolta alle eccellenze con una **formazione specifica in alcuni settori**, tra cui le discipline umanistiche, economiche, giuridiche, e internazionali. Così come rientrano anche le figure tecniche con elevate conoscenze linguistiche, che abbiano capacità di analisi, o esperienze maturate in aree, organizzazioni e/o organismi esteri.

Inoltre, a sostegno delle più recenti iniziative avviate dal governo in materia di protezione cibernetica e sicurezza informatica nazionali, la selezione include profili con qualificate competenze nei vari ambiti della **cybersecurity**, come ad esempio la ricerca, il **monitoraggio, l'analisi ed il contrasto alla minaccia cyber.**

Per presentare i curricula bisogna registrarsi nella pagina Lavora Con Noi di sicurezzanazionale.gov.it. Per candidarsi c'è tempo fino alle 12:00 del **10 maggio 2019**.

https://www.key4biz.it/cybersecurity-tofalo-difesa-presto-defiscalizzazioni-per-le-pmi/253439/

The One Cybersecurity Risk You're Probably Not Even Thinking About

Printers may be the last thing on your mind, but they're a vulnerable point of entry.

April 4, 2019 6 min read

Opinions expressed by *Entrepreneur* contributors are their own.

In November 2018, people took to Twitter to post pictures of a bizarre message regarding a YouTube popularity contest. As it turned out, thousands of internet-connected printers across multiple countries had been hacked — each delivering the same unsolicited printout urging people to subscribe and spread the word about the YouTube competition.

The hacker who claimed responsibility for the stunt said he was trying to teach people a lesson about printer security.

The incident showed just how easy it can be to penetrate a modern printer. Luckily, the hacker didn't have anything in mind more malicious than simply trying to increase a YouTube personality's subscription numbers.

Still, the hacker made a good point, because for most people, printer security is an afterthought; these devices might be the most overlooked high-tech item at businesses today. But the reality is that modern printers are powerful, network-connected devices which carry many of the same vulnerabilities — and liabilities — as any other network computer.

Related: Why Your Innocent Office Printer May Be a Target For Hackers

An overlooked security risk

According to a report by IBM Security and Ponemon Institute, the total cost from security breaches rose by more than 6 percent between 2017 and 2018. And that figure reflects how, for many organizations, exposure of sensitive information can be catastrophic.

Companies waking up to this danger might rush to reinforce workstation and network security while at the same

time overlooking other connected devices such as … printers.

The problem hidden in an easy-access printer

By default, printers are typically set up for easy access and configuration on a corporate network. This default state may be convenient, but it also leaves printers vulnerable to outsiders – and not all hacks are harmless pranks.

A poorly secured printer can actually allow hackers to view documents, steal intellectual property or other sensitive information, print anything they like or inject malware – potentially leading to even worse consequences down the road.

Fortunately, there are ways to manage your organization's printer security risks, and one of them might surprise you: a reliance on cloud services. Here are three strategies to help get the job done:

1. Trust the big names.

Storing potentially sensitive data in the cloud might feel like handing over your newborn baby to a complete stranger, but even the most reluctant old-school IT pros are starting to get it: Storing data in the cloud is more like keeping money in a bank rather than under your mattress.

This version of "the bank" may be less familiar than your bed, but it has vastly superior security and a team of people dedicated to protecting what's yours. Should something go wrong, the burden will not be on you.

As any CEO can attest, corporate cybersecurity is a complex and expensive war that never ends. Guaranteeing the integrity of data – to the greatest extent possible – requires significant resources and the best and brightest security

technologists.

The major cloud application service providers are Amazon Web Services, IBM Cloud, Microsoft Azure and Google Cloud Platform – with AWS currently leading the pack on adoption rates, according to the *2019 State of the Cloud* report. Nobody is likely to outspend these companies on security-related technologies and methods, so that's where you should put your trust.

A private data center is a singular entity: a target with a location and IP ranges. But a secure native cloud platform managed by any of these huge companies is not fixed to a location. It's like spreading your data across multiple buildings far and wide, each with its own security measures right out of *Mission: Impossible*.

Related: 10 Ways to Keep IT Systems Secure

2. "Pack up" and lock down for your move to the cloud.

The transition to cloud services is easy. The process – connecting with your service provider and configuring your printing infrastructure with the cloud – happens in a matter of hours, often less. However, gathering information and *planning* for the move takes a little more work.

For starters, you should put a security policy in place for all network devices (including printers) and ensure that all employees are well versed in that policy. Last year, an independent review of the Kansas Secretary of State's office revealed that two printers had not been properly secured, and neither was password-protected. During a penetration test, a security firm was able to infiltrate the entire government domain right down to the level of those printers.

Experience tells us an effective transition strategy must

first plug such holes. It should also include configuring built-in device firewalls, shutting down unnecessary ports and protocols and developing a firmware-update schedule.

Related: 3 Simple Precautions for Protecting Your Personal Data in the Cloud

IT teams should further educate other employees to guard against attacks. If a hacker tries to infiltrate a company's printer network and fails, other tactics may follow, such as email scams or other forms of direct contact.

3. Use security as a launchpad for more digital improvements.

By design, secure office printing is meant to simplify work for IT professionals: Instead of a company's system having to manage multiple print queues and map employees to various printers, only one virtual print queue will be needed to serve everyone. And securing new devices in your environment can be done with a few clicks.

A study by Oracle predicted that by 2020, 67 percent of organizations will interact with customers through cloud-supported mobile apps, and 87 percent will deliver a multichannel experience. By shifting IT burdens to cloud services — especially in areas such as printing, which is not commonly the domain of in-house expertise — IT teams can spend more time focusing on core business operations.

When adopting cloud services, take advantage of all the new possibilities that not only protect sensitive information, but also ease the burden of routine maintenance and regulatory compliance.

For many organizations, their printing system is the weakest link in an otherwise reliable chain of security. The good news? It's simple to reinforce. With some consulting and a

little prep work, you'll have the flexibility and freedom to focus on your core business while trusting the best-in-class cloud platforms to safeguard your data.

https://www.entrepreneur.com/article/331713

'Il nemico inconfessabile', perché leggere il libro di Paolo Persichetti e Oreste Scalzone

*La rubrica **AssetProtection**, ovvero Riflessioni su sicurezza e terrorismo, a cura di Anthony **Cecil Wright**, presidente Anssaif (Associazione Nazionale Specialisti Sicurezza in Aziende di Intermediazione Finanziaria). Per consultare gli articoli precedenti **clicca qui**.*
Articolo a cura di Carla Capobianchi

"Il nemico inconfessabile" è il titolo di un piccolo volume pubblicato nel 1999, la cui lettura non può lasciare indifferenti perché, attraverso una narrazione densa e serrata, ci costringe a guardare il lungo periodo di sovversione sociale, che ha contrassegnato il nostro Paese dagli anni '60 agli inizi degli anni '80, con gli occhi di due protagonisti della lotta armata di quegli anni, **Paolo Persichetti** e **Oreste Scalzone.**

L'approccio ai fatti, assolutamente controcorrente, spalanca le porte di un capitolo ritenuto dai più definitivamente chiuso, stimolando lo spirito critico ed un'attenta riflessione da parte del lettore.

Considerato che la Francia, in applicazione della dottrina **Mitterand**, ha offerto asilo politico a molti protagonisti degli anni di piombo il volume, come ci viene spiegato nella nota editoriale, è principalmente rivolto al popolo francese, nell'intento di spiegare le ragioni, non compiutamente comprese, del carattere di lotta armata assunto dal movimento sovversivo italiano di quegli anni. Si rivolge tuttavia anche al popolo italiano, al fine di indurlo a riflettere sull'avvenuta negazione da parte dello Stato del carattere, puramente politico, di lotta di classe, o ancor più di guerra civile, che caratterizzò, secondo gli autori, la sovversione sociale propria di quel periodo.

Gli autori, in realtà, sono dei vinti, i protagonisti di una rivoluzione sconfitta, ma, nonostante ciò, espongono le proprie tesi con dovizia di argomentazioni e senza ripensamenti, nella convinzione che uno scontro così violento fosse inevitabile in una situazione di contrasto insanabile fra le politiche "accomodanti" imposte dal sistema e la dinamicità del contesto sociale.

Infatti, secondo gli autori, si sarebbe trattato di una vera e propria rivoluzione, in cui furono coinvolti strati sociali massicci della popolazione italiana, giovani, operai, disoccupati, donne, e quindi di un movimento di massa dalle enormi potenzialità, capace di destabilizzare, con il proprio impeto, l'ordine costituito.

Gli autori si soffermano quindi sulla reazione che tale movimento suscitò nella società politica per la quale, negli anni del "compromesso storico" e dei governi "di unità nazionale", la guerra sociale in corso rappresentò un "nemico inconfessabile", da cancellare e rimuovere. Fu così che fu instaurato uno "stato di emergenza permanente", dissimulato "sotto l'apparente aspetto della normalità giuridica",

disconoscendo la connotazione politica della rivolta.

In conclusione, **Scalzone** e **Persichetti** auspicano l'avvento di una soluzione politica per i "ribelli" degli anni di piombo, in un'ottica rivolta anche al futuro dei movimenti sociali che verranno.

Una serie di "Appendici" completano l'opera, approfondendo alcuni aspetti ed offrendo così ulteriori spunti di riflessione al lettore. Fra le altre quella che affronta la questione, di scottante attualità, dei fuoriusciti italiani che hanno trovato rifugio in territorio francese, recante il testo di una lettera aperta, indirizzata al Presidente della Repubblica **Chirac** ed al Primo Ministro **Jospin** e pubblicata su **Le Monde** nel 1998, dalla quale si evince con chiarezza il punto di vista degli espatriati italiani sulla situazione da essi vissuta e sulle possibili decisioni da assumere nei loro confronti.

Articolo a cura di Carla Capobianchi

> *'Il nemico inconfessabile', perché leggere il libro di Paolo Persichetti e Oreste Scalzone*

Spyware Exodus, Soro: 'L'utilizzo dei software spia va disciplinato in modo molto

più rigido’

Il Garante per la protezione dei dati personali, **Antonello Soro**, ha spiegato le preoccupazioni emerse dalla vicenda dello **Spyware Exodus,** – software utilizzato da molte procure italiane per spiare legalmente i criminali – finito per ‘sbaglio’ nel Play Store di **Google** e che ha intercettato per errore cittadini non oggetto di indagini.

“*L’utilizzo di captatori informatici, cioè di software spia che vengono utilizzati per attività investigative da parte della magistratura sono uno strumento tecnologicamente molto avanzato e molto invasivo che da alcuni anni viene utilizzato all’interno di una disciplina non stringente* **–** ha detto Soro ai microfoni di **Radio 24.**

“Abbiamo più volte sollecitato ai vari Governi una definizione più puntuale delle regole e delle misure di sicurezza proprio perché la potenzialità di questo software, una volta che abbia infettato il dispositivo telefonico o il computer di una persona è capace di diventare un arma letale in quanto non si limita solo nelle comuni intercettazioni telefoniche, ma segue la persona coinvolta in tutte le tue relazioni”.

“La legge” – ha spiegato Soro – *“prevede che il magistrato dispone l’utilizzo di un captatore nei confronti di una persona sospettata di reati importanti. Questo procedimento viene affidato alla polizia giudiziaria che a sua volta utilizza soggetti o gestori con competenze tecnologiche varie. Questo è uno degli aspetti che da tempo abbiamo sottolineato come pericoloso in quanto ogni procura per tutte le intercettazioni ha la possibilità di rivolgersi a gestori del territorio più o meno affidabili. Ma proprio per questo un’arma così importante in una architettura che coinvolge troppi soggetti, la catena di responsabilità si allunga e il rischio di un incidente come quello che si è verificato cresce esponenzialmente”.*

“Noi diciamo da tempo che questa catena va accorciata” – ha aggiunto il Garante Privacy –, *“perché l’utilizzo dei captatori deve avvenire se è possibile all’interno di competenze interne allo Stato, alla magistratura, alla polizia giudiziaria proprio per non comportare il rischio che persone del tutto estranee alle indagini vengono coinvolte in una raccolta massiva di informazioni”.*

“L’utilizzo dei captatori” – ha concluso Antonello Soro – *“va disciplinato in modo molto più rigido. Una sollecitazione che noi abbiamo rivolto da tempo, e non si capisce perché ancora non è stato fatto nulla. Pensiamo che le intercettazioni di qualunque genere siano uno strumento potentissimo di cui la polizia e la magistratura devono disporre, ma lo devono fare all’interno di una cornice di garanzie per i cittadini con misure di sicurezza informatiche e organizzative molto severe.*

https://www.key4biz.it/spyware-exodus-soro-lutilizzo-dei-software-spia-va-disciplinato-in-modo-molto-piu-rigido/252455/

Cyber-intelligence, nasce Memento Labs dalla fusione delle attività di InTheCyber Group e la storica Hacking

Team

IntheCyber Group ha acquisito la società Hacking Team dal precedente proprietario David Vincenzetti, suo CEO e fondatore. Nasce quindi **Memento Labs** nella quale si concentreranno le attività di cyber-intelligence di IntheCyber Group e le attività della precedente Hacking Team.

"In questo modo viene effettuata, di fatto, una Segregation of Duties (SoD) tra le attività del Gruppo", ha dichiarato a Key4biz, **Paolo Lezzi**, Presidente di Memento Labs e CEO and Founder di InTheCyber Group, *"i servizi di Cyber Security avanzata continueranno ad essere prerogativa delle società operative IntheCyber Srl ed IntheCyber Suisse, ed erogate nei confronti di aziende ed istituzioni, mentre verrà accuratamente rilanciata con Memento Labs tutta la realizzazione di tool e piattaforme per le attività di Law Enforcement ed Intelligence, soprattutto in un momento come questo, dove la sofisticazione tecnologica della criminalità internazionale e delle attività terroristiche porta ad una necessità di assoluta attenzione da parte delle realtà istituzionali nello svolgere le proprie attività investigative. Si vedano, ad esempio, gli ultimi fatti accaduti con Exodus".*

Key4biz. ***Di nuovo riflettori puntati su Hacking Team, ma per ordinari interessi di mercato. E lei è il cavaliere bianco che ha deciso di acquistare società e competenza. Perché?***

Paolo Lezzi. È assolutamente necessario che in Italia esista, quindi che permanga e venga rilanciata, una realtà di R&D con competenze esclusive a livello internazionale, soprattutto in un momento in cui tanti attori si affacciano – anche in maniera non troppo professionale – a una attività che richiede la massima professionalità, attenzione ed eticità.

Key4biz. ***Cos'è che l'ha spinta a questo passo? Ragioni di mercato, congiunture internazionali, ruolo dell'Italia o cos'altro?***

Paolo Lezzi. Sarebbe stato un vero peccato disperdere delle competenze esclusive presenti in Hacking Team come pure rischiare di farle diventare di proprietà di attori stranieri. Questa nuova realtà, per come si configura sia per il profilo del Gruppo IntheCyber sia per il posizionamento che avrà Memento Labs, la candida ad essere uno dei principali attori a livello mondiale in questo settore.

L'Italia può fare la differenza, il nostro Paese ha una storia di capacità creativa e di innovazione tecnologica dovuta alla sua cultura e alle sue università che va valorizzata e difesa.

La nuova Memento Labs è composta da 50 persone, con una cospicua presenza di giovani che, in questo momento di rilancio, potrà trovare ulteriori spazi per nuove leve e collaborazioni con i laboratori di ricerca universitari.

Abbiamo acquisito questa società perché vogliamo fortemente che resti italiana, dando valore ai giovani talenti ed evitando che vadano via. Infatti, è solo da una stretta collaborazione pubblico-privata e accademica che si può far evolvere la sicurezza nazionale.

Key4biz*. Quell'Hacking Team non esiste più oggi o sbagliamo? Le sue attività si sono fermate effettivamente al 2016 dopo le note vicende internazionali o hanno proseguito in altre direzioni? In genere quando si acquisisce una società si rileva ovviamente anche il portafoglio clienti, ma nel caso di Hacking Team, vi era una attività ed un portafoglio clienti in piedi?*

Paolo Lezzi. I clienti di Memento Labs, come erano quelli di

Hacking Team, sono e saranno sempre e solo esclusivamente clienti governativi e quindi realtà di *intelligence* e realtà di *Law Enforcement* che necessitano di tecnologie avanzate di supporto allo svolgimento di moderni processi investigativi. Le capacità della unità di R&D ha continuato ad essere stimata ed apprezzata a livello internazionale e da questo ripartiamo.

Key4biz. ***Quanto peserà la vecchia eredità di un logo così, diciamolo pure, ingombrante? Pensa di dar luogo ad un re-branding o ad una rigenerazione del vecchio marchio?***

Paolo Lezzi. È un totale re-branding. Memento Labs è, a tutti gli effetti, una nuova società che prenderà il meglio di Hacking Team insieme al meglio delle capacità di cyber-intelligence di IntheCyber Group.

Memento Labs valorizzerà tutti gli aspetti positivi di una importante eredità, incentivandone la percezione positiva di eccellenza nelle competenze tecniche e R&D per offrire soluzioni a supporto della lotta al Crimine e della Sicurezza Nazionale

Per saperne di più: cyber

> *Cyber-intelligence, nasce Memento Labs dalla fusione delle attività di InTheCyber Group e la storica Hacking Team*

Spyware Exodus, i dati trovati in server all’estero.

Chi ha avuto accesso?

Tanti risvolti nella storia di **Exodus**, il malware tutto italiano che ha rubato informazioni a più di 1000 utenti, in Italia.

L'inchiesta della procura di Napoli ha accertato come migliaia di messaggi, foto, video, chat e conversazioni intercettate – sia di persone indagate per conto delle procure, sia di ignari cittadini illecitamente spiati dal malware – sia finito all'estero, senza alcune protezione, in un server di **Amazon** in **Oregon**.

La Procura di Napoli ha messo sotto indagine quattro persone e ottenuto dal Gip il sequestro di due società, la **eServ** srl di Catanzaro e la **Stm srl**.

Tutto ruotava intorno al sistema spyware **Exodus**, realizzato da eSurv e commercializzato dalla Stm. Uno strumento in dotazione agli inquirenti di numerose Procure con il quale era possibile tenere sotto controllo le attività telematiche degli indagati.

Violazione della privacy

I dati sono "disponibili a chiunque ne conosca le coordinate senza controlli o limiti". Adesso le indagini puntano a stabilire in quanti e con quali fini abbiano avuto accesso alla piattaforma Exodus. Di certo sulla piattaforma, come precisano gli inquirenti sono disponibili *"Imei riconducibili a procedimenti penali, Imei in uso ad altri organi di polizia giudiziaria ed Imei in uso a persone da identificare".*

Inoltre ad avere accesso erano le società che avevano stipulato accordi di commercializzazione e impiego del

software Exodus, che secondo gli inquirenti sono circa una ventina.

Quattro indagati

Le informazioni giudiziarie, però, invece di essere stoccate nelle unità di storage, venivano trasferite su un'area cloud di Amazon, illegalmente di esclusivo appannaggio della e-Surv.

I quattro indagati sono il rappresentante legale e l'amministratore di fatto di Stm srl, e l'amministratore legale e il direttore delle infrastrutture It di e-Surv. A tutti vengono contestati, tra l'altro, la violazione delle norme sul trattamento dei dati personali e la frode in pubblica attività.

Cosa può fare Exodus

Lo spyware è in grado di effettuare numerosissime operazioni sul telefono della vittima, perché studiato appositamente per spiare, dato che il software è stato sviluppato come parte di un progetto finanziato dalla **Polizia di Stato**, destinato appunto all'impiego nelle indagini.

Il malware può registrare le telefonate, l'audio ambientale, copiare gli sms e i numeri di telefono in rubrica e leggere la posizione attraverso il gps.

Nono solo privacy

L'accusa ovviamente è quella di violazione della privacy, ma il sospetto evidente è che siano servite anche a svolgere attività di dossieraggio e di ricatto.

Uno degli indagati ha dichiarato di aver inondato la rete col malware spia per fare dei semplici 'test'. Il pericolo però, che non si sa quante persone o addirittura aziende hanno avuto

accesso ai dati.

https://www.key4biz.it/spyware-exodus-i-dati-trovati-in-server-allestero-chi-ha-avuto-accesso/252354/

Sicurezza e terrorismo, Valter Giovannini: 'In Italia reati diminuiti, ma la percezione di insicurezza è ancora alta'

*La rubrica **AssetProtection**, ovvero Riflessioni su sicurezza e terrorismo, a cura di Anthony **Cecil Wright**, presidente Anssaif (Associazione Nazionale Specialisti Sicurezza in Aziende di Intermediazione Finanziaria). Per consultare gli articoli precedenti **clicca qui**.*

Oggi abbiamo il piacere di avere con noi il dott. **Valter Giovannini** (Sostituto Procuratore Generale presso la Corte d'Appello di Bologna dopo avere fatto parte per circa sette anni della Direzione Distrettuale Antimafia della Procura di Bologna ed essere stato, per otto anni, Procuratore Aggiunto presso il medesimo ufficio) che, oltre ad essere un affezionato lettore fin dal primo numero della nostra newsletter, è un nostro graditissimo interlocutore.

Pietro Blengino: ***Dott. Giovannini, innanzitutto grazie per aver accettato la nostra richiesta di un'intervista. Lei fa il Pubblico Ministero da circa 35 anni e nella sua carriera si è occupato di molteplici fenomeni criminali. Dal 1994, vive e lavora a Bologna dove il fenomeno del '68 (su cui nei nostri***

numeri abbiamo soffermato la nostra attenzione) ha manifestato insieme a una fortissima carica innovativa delle derive violente sia a livello di massa (ricordo per tutti quanto accaduto nel '77 a Bologna) sia a livello di gruppi terroristici organizzati. Per questo motivo vorremmo sapere come vede oggi la situazione italiana dal punto di vista della sicurezza.

Valter Giovannini. Le statistiche, che peraltro non sempre fotografano con assoluta precisione la realtà, ci dicono che il numero complessivo dei reati è in diminuzione. Tuttavia tra la gente è sempre alta la percezione di insicurezza e questo sentimento deve essere rispettato e mai criticato.

Pietro Blengino. ***E del terrorismo?***

Valter Giovannini. Abbiamo i nostri servizi di intelligence e quelli di polizia giudiziaria che operano sul territorio impegnati al massimo nell'azione di prevenzione e contrasto di un fenomeno assai variegato. Oltre a possibili iniziative criminali riconducibili all'estremismo di matrice religiosa non dobbiamo mai dimenticare che nel nostro paese, da anni, l'anarcoinsurrezionalismo ha dichiarato una guerra per il momento di "bassa intensità" allo Stato; fatta di attentati incendiari a sedi di enti economici pubblici o privati e al sistema delle telecomunicazioni.

Poi è sempre in auge il criminale utilizzo delle buste contenenti esplosivo, inviate a mezzo posta a persone che costoro hanno individuato come avversari politici.

Pietro Blengino. ***In cosa si differenzia l'odierna minaccia rispetto a quella che abbiamo conosciuto in passato?***

Valter Giovannini. Sicuramente nel nostro passato l'originario ribellismo ha virato, nel corso degli anni, in

forme violente di stampo terroristico. I fondatori delle Brigate Rosse agivano in nome del mito “della resistenza tradita”. L’estremismo di destra agiva perché vedeva un nemico non solo nell’avversario politico ma anche nei rappresentati di uno Stato percepito, da un certo momento in avanti, come un bieco repressore. Certo è che entrambe le parti hanno versato troppo sangue innocente intossicando la società per decenni. Oggi, al momento, la situazione non è paragonabile; è per così dire molto fluida. Penso però che non sia immaginabile quel consenso, sotto traccia che, purtroppo, in alcuni ambienti ci fu negli anni più violenti del terrorismo.

Pietro Blengino. Le pongo una domanda che spero non sia fonte di difficoltà. Quali sono le iniziative che potrebbero essere messe in atto per migliorare la prevenzione? Ricordo che parlammo alcuni mesi fa di una sua visita a Strasburgo in cui lei mi raccontò le diverse misure di prevenzione messe in atto dalle locali Forze dell’Ordine. Purtroppo, a dicembre abbiamo dovuto assistere a un grave fatto di sangue proprio a Strasburgo. Che indicazioni ha tratto anche dalla sua esperienza personale?

Valter Giovannini. Penso che sia giunto il momento, per noi europei, di porci, senza steccati ideologici, la domanda: è ancora possibile pretendere il massimo delle libertà individuali e collettive unitamente al massimo della sicurezza possibile? Se la risposta è che non siamo disposti a rinunciare neppure a controlli a campione di natura preventiva, ad esempio sulla rete web, allora, onestamente, dobbiamo ammettere che siamo disponibili a correre ulteriori rischi di utilizzo distorto della rete da parte di chi, pur richiamandosi a modelli sociali vecchi di millenni, utilizza i più moderni sistemi informatici per divulgare i propri proclami di guerra, tenere contatti tra gli accoliti e creare proseliti.

Pietro Blengino. ***Continuando il tema toccato dalla precedente domanda mi soffermo su un punto. Negli anni ’70 per il***

contrasto del terrorismo furono sicuramente importanti gli interventi messi in atto dalle Forze dell'Ordine e dalla Magistratura ma sicuramente fu importante il ruolo che la classe politica e la popolazione ebbero nel far mancare al terrorismo quell'humus favorevole di cui aveva inizialmente goduto. Cosa manca oggi?

Valter Giovannini. Personalmente credo che negli anni ottanta il terrorismo oltre ad essere stato contrastato con grande efficacia dalle forze dell'ordine e dalla magistratura, che per questo hanno pagato grandi tributi di sangue, è imploso per cause interne. La spinta propulsiva è venuta meno quando il furore ideologico è stato prima affiancato e poi sostituito dalla consapevolezza di un totale fallimento umano e politico del progetto insurrezionale o eversivo.

Pietro Blengino. ***E dal punto di vista tecnico giudiziario?***

Valter Giovannini. Abbiamo un tessuto normativo assolutamente adeguato a contrastare e reprimere qualsiasi fenomeno criminale. Rimane però fondamentale la collaborazione da parte di noi tutti nel segnalare fatti ed episodi che potrebbero essere sintomatici di attività criminali anche molto gravi. Penso, come esempio, alla possibilità astratta che un giovane, apparentemente inserito nel contesto sociale, inizi ad assumere atteggiamenti sintomatici di una qualche forma di radicalizzazione. Chi è vicino a lui, e non ne condivide le scelte, non può non accorgersi di quanto stia accadendo. Ecco, nell'interesse di tutti a cominciare dal giovane che forse è attirato da sirene estremistiche, sarebbe meglio trovare il modo di segnalare, anche in forma riservata, quanto sta accadendo. Il risultato positivo potrebbe essere duplice: impedire la commissione di reati e di conseguenza recuperare anche il potenziale estremista. Non sarebbe delazione ma sana collaborazione alla gestione corale di una società estremamente complessa quale quella in cui noi tutti viviamo.

diminuiti, ma la percezione di insicurezza è ancora alta’

Cybersecurity, l’Intelligence italiana cerca giovani analisti ed esperti cyber

Al via da oggi **fino al prossimo 10 maggio** il **reclutamento mirato dell’Intelligence italiana**.

Le nuove opportunità sono soprattutto rivolte per i giovani interessati a far parte del personale del Comparto Intelligence e che intendono dare un concreto contributo alla missione del **DIS**, dell’**AISE** e dell’**AISI** a tutela degli interessi strategici nazionali in campo politico, militare, economico, scientifico e industriale.

Si tratta di un’occasione che chiede ai giovani anche – spiega la nota del Ministero – una sentita adesione ai valori che caratterizzano il Sistema di informazione della sicurezza della Repubblica, tra cui la lealtà, la riservatezza, il coraggio, il segno di patriottismo, la proiezione verso il futuro.

A chi si rivolge

La ricerca è rivolta alle eccellenze con una **formazione specifica in alcuni settori**, tra cui le discipline umanistiche, economiche, giuridiche, e internazionali. Così come rientrano anche le figure tecniche con elevate conoscenze linguistiche, che abbiano capacità di analisi, o esperienze

maturate in aree, organizzazioni e/o organismi esteri.

Inoltre, a sostegno delle più recenti iniziative avviate dal governo in materia di protezione cibernetica e sicurezza informatica nazionali, la selezione include profili con qualificate competenze nei vari ambiti della **cybersecurity**, come ad esempio la ricerca, il monitoraggio, l'analisi ed il contrasto alla minaccia.

I curricula disponibili all'esito dell'attività di ricerca saranno sottoposti alle previste **procedure selettive**, articolate in un preliminare screening delle candidature arrivate, ed una seconda fase in cui vengono verificati i profili di professionalità, affidabilità e sicurezza dei candidati.

Dove presentare domanda

Questo avviso di ricerca **non è l'unico dei canali di reclutamento** consentiti dalla legge di riforma del Comparto: per tutti gli altri profili, infatti, rimane attiva la possibilità di presentare candidature spontanee attraverso la sezione del sito **Lavora con noi**. Così come attivo resta lo scouting presso gli Atenei nazionali per neolaureati che hanno chiuso gli studi con una votazione apicale.

Per candidarsi c'è tempo fino alle 12:00 del **10 maggio 2019**

https://www.key4biz.it/cybersecurity-lintelligence-italiana-cerca-giovani-analisti-ed-esperti-cyber/252286/

Exodus, tutta la storia dello spyware made in Italy

Per circa due anni qualcuno ha distribuito **malware** in grado di colpire i dispositivi delle vittime non solo esponendo le informazioni in essi contenute, ma anche rendendoli vulnerabili ad attacchi perpetrati da parte di terzi.

E’ la storia di **Exodus**, un malware tutto italiano che ha rubato informazioni a più di 1000 utenti, in Italia.

Sviluppato dalla società calabrese **eSurv**, che produce soluzioni per la sorveglianza, avrebbe intercettato per ‘errore’ persone non indagate.

Indagate perché questo speciale sypware è stato creato apposta per spiare persone finite sotto inchiesta, dato che il software è stato sviluppato come parte di un progetto finanziato dalla **Polizia di Stato**, destinato appunto all’impiego nelle indagini.

Scoperto dalla società **Security without borders** in collaborazione con **Motherboard,** la società si è difesa dichiarando che con **Exodus** è stato diffuso per errore sul Play Store di **Google**.

Cosa può fare Exodus

Lo spyware è in grado di effettuare numerosissime operazioni sul telefono della vittima, perché studiato appositamente per spiare i criminali. Può registrare le telefonate, l’audio ambientale, copiare gli sms e i numeri di telefono in rubrica e leggere la posizione attraverso il gps.

In seguito alla scoperta, Security without borders ha segnalato a Google la presenza dello spyware, che è stato rimosso in tutte le sue varianti, circa 25.

Antonello Soro (Garante Privacy): 'Fatto Gravissimo'

"*È un fatto gravissimo* – ha dichiarato **il Garante della Privacy Antonello Soro** – *su cui c'è grande preoccupazione. Faremo i dovuti approfondimenti per quanto concerne le nostre competenze, poiché la vicenda presenta contorni ancora assai incerti ed è indispensabile chiarirne l'esatta dinamica*".

Una storia dai contorni in massima parte ancora oscuri che rilancia l'allarme sul "far west" delle intercettazioni di Stato.

Il commento di Angelo Tofalo (Sottosegretario alla Difesa)

" *Se i fatti contestati risultassero aderenti alla realtà, rappresenterebbero l'ennesima pericolosa devianza nell'utilizzo di strumenti non sufficientemente monitorati da una politica poco sensibile alla gestione del dominio cibernetico*". Ha dichiarato il sottosegretario alla Difesa **Angelo Tofalo** commentando l'indagine e dicendosi "*fiducioso che la magistratura intraprenderà al meglio la propria azione accertando tutte le responsabilità, confidando sul fatto che nessuna istituzione abbia mai fatto un uso illecito del malware* ***Exodus***".*Non ci resta – aggiunge il sottosegretario – che sperare che gli investimenti in uomini e mezzi attivati in questi mesi possano contenere altre vulnerabilità di cui non abbiamo ancora evidenza*".

Il commento di Deborah Bergamini (FI)

“*Sarebbe intollerabile scoprire che nello Stato qualcuno abbia potuto accedere, in maniera ingiustificata, a delle comunicazioni private violando l’articolo 15 della Costituzione. Chiederemo che venga fatta chiarezza sullo spyware Exodus e continueremo a chiedere con forza che venga istituita una Commissione parlamentare di Inchiesta sull’utilizzo dei dati degli utenti”.* Ha scritto su Facebook l’on. **Deborah Bergamini**, Vicepresidente e responsabile della Commissione Trasporti, Tlc e Poste di **Forza Italia.**

Chi non capisce che dalla sicurezza dei dati passa il futuro della democrazia, – conclude la deputata su Fb – rischia di rimanere confinato ai margini della storia“.

Azienda sotto sequestro

Intanto la Procura di Napoli ha chiesto e ottenuto il sequestro preventivo della società. Si indaga per scoprire come sia stato possibile che un’applicazione, destinata ad essere utilizzata solo su richiesta e sotto il controllo della magistratura, fosse disponibile on line su “Google store”, così da ingannare ignari utenti che l’hanno scaricata sui loro cellulari e si sono ritrovati illecitamente spiati.

https://www.key4biz.it/exodus-lo-spyware-made-in-italy-finito-per-sbaglio-sul-play-store-di-google/252144/

Cloud e data center nel mirino degli hacker. In aumento attacchi DDoS a livello globale

La digital transformation è una strategia fondamentale per le aziende che intendono cogliere nuove opportunità di guadagno, ma fa sì che questi nuovi servizi attirano l'attenzione dei criminali informatici, che hanno iniziato a colpirli con sempre maggiore frequenza.

A dirlo è il rapporto annuale sulla sicurezza delle infrastrutture mondiali di **Netscout,** giunto alla quattordicesima edizione, un documento che contiene importanti informazioni sulle sfide operative e di sicurezza affrontate dai service provider e dagli operatori delle reti aziendali in diversi paesi del mondo.

Secondo lo studio a farla da padrone sono gli attacchi **DDoS** (***Denial of Service),*** attacchi informatici in cui si fanno esaurire deliberatamente le risorse di un sistema informatico che fornisce un servizio ai client, ad esempio un sito web su un web server, fino a renderlo non più in grado di erogare il servizio ai client richiedenti.

Nel 2018, spiega il report, l'entità degli attacchi DDoS ha subito un'impennata raggiungendo il livello record di 1,7 Tbps, mentre continuano a evolversi nuovi bersagli e nuove tecniche.

Gli attacchi DDoS continuano a crescere

Il report in particolar modo evidenzia:

- Il 91% delle aziende colpite da un attacco DDoS ha dichiarato che uno o più attacchi hanno saturato completamente la banda Internet.
- I criminali informatici si sono concentrati maggiormente sugli attacchi alle infrastrutture stateful, colpendo firewall e dispositivi IPS. Questi attacchi sono quasi raddoppiati, passando dal 16 al 31%.
- Tra i soggetti colpiti dagli attacchi stateful, il 43% ha riferito che il firewall e/o il dispositivo IPS ha contribuito a un'interruzione durante l'attacco.
- Il 36% delle aziende ha subito attacchi multivettore complessi mirati alla banda, all'infrastruttura stateful e alle applicazioni.

Gli ingenti costi dei tempi di inattività

Nel 2018, il costo globale medio di un'ora di inattività associata alle interruzioni dei servizi Internet causate dagli attacchi DDoS ammontava a 221.836,80 dollari. Il costo più elevato, registrato in Germania, corrisponde a 351.995 dollari. In Giappone, un'ora di inattività della rete ammonta invece a 123.026 dollari.

Chi sono le vittime preferite del cybercrime

- **Servizi SaaS**

Gli attacchi DDoS contro i servizi SaaS sono triplicati

rispetto all’anno precedente, passando dal 13 al 41%.

- **Data center e servizi cloud esterni**

Anche in questo settore, gli attacchi DDoS sono triplicati rispetto all’anno precedente, passando dall’11 al 34%.

- **Attacchi al traffico crittografato**

Il crescente utilizzo del traffico crittografato si riflette nella maggiore percentuale di attacchi mirati contro questo tipo di traffico. Nel 2018, il 94% degli intervistati ha osservato attacchi di questo genere, in quantità quasi raddoppiate rispetto all’anno precedente.

- **Service provider**

Anche i servizi basati su cloud sono stati maggiormente colpiti dagli attacchi DDoS, con un aumento dal 25% del 2016 al 47% del 2018.

https://www.key4biz.it/cloud-e-data-center-nel-mirino-degli-hacker-in-aumento-attacchi-ddos-a-livello-globale/251659/