Tutti sono concentrati sul GDPR, per evitare le multe. Ma chi investe in una maggiore resilienza?

*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**.*

Il mio precedente articolo ha stimolato alcuni a fornirmi un loro feedback: sono stati tutti di approvazione di quanto da me affermato.

Fra questi, segnalo e riporto qui di seguito, in forma schematica, quanto segnalatami da una persona di lunga esperienza ed elevata competenza:

1. Diffuse carenze nella consapevolezza sulla gestione dei rischi, specialmente informatici;
2. Scarse e poco autorevoli figure nell'ICT;
3. Cattive prassi consolidate;
4. Tendenza ad occultare la presenza di rischi e criticità;
5. Diffuse scarse competenze culturali ed informatiche;
6. Poca meritocrazia;
7. Insufficiente budget dedicato alla protezione cyber;
8. Insufficiente formazione necessaria a creare la corretta consapevolezza nell'utilizzo della dotazione informatica.

Ho letto e riletto diverse volte quanto scritto da questa persona, che ricopre tra l'altro un ruolo apicale in una grande azienda, ed ho concluso che a mio avviso si sia rappresentata una situazione reale.

Ho voluto comunque sentire il parere di altri manager che si occupano di information security, operational risk management, ed auditing.

Tutti hanno condiviso quanto scritto.

La situazione è davvero grave, e, quindi, che fare?

Un collega mi ha detto: «Se rifletti, ora tutti sono concentrati sul GDPR: perché? Perché ci sono penalità molto elevate. Ma quante organizzazioni hanno investito e stanno investendo in una maggiore resilienza? Quante si sono accontentate di qualche procedura ad hoc, nuove disposizioni interne e la responsabilizzazione dell'outsourcer? Nemmeno il rischio di attacchi cyber da concorrenti, nazioni nemiche o da gruppi terroristici, che possano mettere in crisi l'azienda, mettono paura. Bisogna allora puntare sui giovani: creare in loro la giusta consapevolezza dei rischi.».

Riassumendo, il consiglio è: penali elevate e "awareness" nei più giovani?

Concludo con una frase tratta dal lungo testo pervenutomi, e che ha trovato il maggior consenso fra i colleghi:

«Purtroppo l'insufficiente etica professionale, unitamente a scarse competenze culturali ed informatiche, anche ai livelli più alti, riducono l'efficienza interna e quindi la competitività della singola azienda e del Sistema Paese. La poca meritocrazia, permette a persone inadeguate di ricoprire ruoli direttivi, compromettendo un sano processo decisionale, la motivazione delle risorse ed il perseguimento di una corretta Governance aziendale. ».

Il security manager sarà sempre più solo? O sarà l'unico a pagare le conseguenze di un riuscito attacco cyber?

Anthony.wright@anssaif.it

https://www.key4biz.it/tutti-sono-concentrati-sul-gdpr-per-evitare-le-multe-ma-chi-investe-in-una-maggiore-resilienza/259419/

Instagram, online su un database non protetto dati di 50 milioni di Influencer

Privacy e social network, ci risiamo. Dati di 50 milioni di utenti, per lo più di influencer e celebrità, sono stati trovati in un database allocato su un serve AWS, **Amazon Web Services,** senza alcuna password di protezione: chiunque poteva entrare e prelevare i dati.

Un nuovo scandalo privacy proveniente dall'Universo **Facebook**, in quanto **Mark Zuckerberg** è proprietario del popolare social network acquistato nel 2012 per la modica cifra di 1 miliardo di dollari.

A fare la scoperta è stata la testata americana **TechCrunch**, dopo essere stata allertata dal ricercatore **Anurag Sen.** Secondo quanto riporto dal quotidiano, l'archivio conteneva i dati di 50 milioni di utenti. Tra i dati che è possibile ricavare tutta la biografia dell'utente, la foto del profilo, il numero di follower, se sono verificati o no, la località (città e nazione) ma anche le informazioni di contatto private, come l'indirizzo email dell'account Instagram e il numero di telefono del proprietario dell'account.

L’azienda proprietaria del database: Chtrbox

Il ricercatore, attraverso le sue rilevazioni, è riuscito a risalire al proprietario del database che è la società **Chtrbox**, con sede a Mumbai, che si occupa di social media marketing e che lavora proprio con gli influencer per pubblicare contenuti sponsorizzati sui loro account. E, infatti, tra i vari dati rintracciati, c’erano anche quelli riferiti alla capacità di influenza di ciascun influencer, in base al numero di follower, capacità di interazione, portata potenziale, “like” e singole condivisioni.

Il secondo episodio in pochi anni

Il database è stato messo offline poco dopo la richiesta di spiegazioni dalla società indiana. Intanto da Facebook, un portavoce ha fatto sapere che la società sta esaminando il problema «per capire se i dati descritti, inclusi i numeri di e-mail e di telefono, provenivano da Instagram o da altre fonti.

Un episodio simile era già avvenuto un paio di anni fa, dopo che era stato scoperto un bug nelle **API** che aveva poi costretto la società di proprietà di Facebook ad attuare una stretta, in modo da limitare le richieste.

https://www.key4biz.it/instragram-online-su-un-database-non-protetto-dati-di-50-milioni-di-influencer/258812/

Europol, smantellata la cyber-gang del malware GozNym

Hanno utilizzato il **malware GozNym** per cercare di rubare qualcosa come 100 milioni di dollari da oltre 41mila vittime. Con quest'accusa, una rete di cybercriminali è stata smantellata da un'operazione coordinata europea di polizia, secondo quanti riferisce ieri **Europol**.

L'indagine condotta in 4 Paesi

La complessa operazione di polizia è stata condotta negli Stati Uniti, in Bulgaria, Germania, Georgia, Moldova e Ucraina. Adesso dieci membri della gang devono rispondere negli Usa a una serie di reati, tra cui il furto di denaro e il riciclaggio attraverso conti bancari statunitensi e stranieri. Tra gli altri membri anche il 'capo' della rete, oltre al suo assistente tecnico, fermati in Georgia.

41mila computer infettati

La gang ha infettato 41mila computer con il malware, che ha catturato i dati bancari online per accedere ai conti correnti delle vittime.

La rete GozNym pubblicizzava le sue capacità di commettere cybercrimini come "un servizio". I componenti del network si presentavano come degli specialisti nel settore nei forum criminali online in lingua russa.

https://www.key4biz.it/europol-smantellata-la-cyber-gang-del-malware-goznym/258592/

Intel, nuova falla di sicurezza nei processori. Gli aggiornamenti per evitare i rischi

Gli utenti malintenzionati hanno avuto la possibilità di accedere facilmente a password o token di accesso dei conti correnti online e a messaggi privati delle vittime, ossia a tutti gli ultimi dati sensibili memorizzati nel processore, ma anche disponibili sul cloud. Questi sono i gravi rischi della falla di sicurezza scoperta in buona parte dei microprocessori **Intel** prodotti a cominciare dal 2011. Come è successo l'anno scorso, quando è stato individuato un altro bug nei processori Intel, Adm e Arm (gli ultimi due ora non sono coinvolti), a intercettare la falla sono stati i ricercatori dell'università tecnica di Graz, in Austria, esperti di cybersecurity, che hanno etichettato la vulnerabilità "Zombie load" o microarchitectural data sampling (**MDS**) per indicare i carichi di dati che la Cpu non riesce a "capire" o a elaborare correttamente. Per evitare un errore, il processore chiede l'intervento del microcode: in questa fase alcune informazioni generate dalle applicazioni in esecuzione potrebbero filtrare al di fuori del perimetro predefinito.

La vulnerabilità scoperta ha sfruttato una debolezza nell'esecuzione speculativa, una parte importante del funzionamento dei processori moderni. **Daniel Gruss**, uno dei ricercatori che ha scoperto la falla, ha detto che i malintenzionati sfruttando la vulnerabilità avrebbero potuto leggere i dati dal processore "proprio come" gli utenti vittime dell'attacco. Infatti, l'attacco "Zombie Load"

avrebbe consentito di rubare dati e chiavi sensibili nel momento di accesso da parte dell'utente.

Intel ha poi rivelato che la falla è composta da 4 bug e ha provveduto a rilasciare le patch per risolvere il problema. Anche **Apple** (solo per i Mac, perché gli altri dispositivi della società non sono interessati dal bag), **Google**, **Amazon** e **Microsoft** hanno rilasciato aggiornamenti per rendere immuni gli attacchi ai loro sistemi operatori a causa della falla nei microprocessori Intel. Mentre Mozilla ha pianificato lo sviluppo di una soluzione a lungo termine.

Sebbene non ci sia stata notizia di nessun attacco sferrato con successo a causa della falla, i ricercatori fanno notare che comunque non avrebbe necessariamente lasciato traccia.

Una considerazione finale. Due giorni fa la scoperta di una grave vulnerabilità di **WhatsApp**, oggi di nuovo su Intel. Ma secondo i funzionari Usa non sono solo le apparecchiature di telecomunicazioni cinesi a non essere sicure?

> *Intel, nuova falla di sicurezza nei processori. Gli aggiornamenti per evitare i rischi*

Cybersecurity nella PA, in consultazione pubblica le

linee guida per i Cert regionali

La sicurezza informatica della PA riveste un'importanza fondamentale perché necessaria a garantire la disponibilità, l'integrità e la riservatezza delle informazioni del Sistema informativo della Pubblica amministrazione assicurando la fiducia, presupposto per la diffusione dei servizi digitali.

Per questo motivo **AgID**ha annunciato che dal 14 maggio al 13 giugno 2019, sono in consultazione le "Linee Guida sulla sicurezza nel procurement ICT" e le "Linee guida per lo sviluppo e la definizione del modello nazionale di riferimento per i CERT regionali", secondo le previsioni dell'art. 14-bis del Codice dell'Amministrazione Digitale.

A cosa servono le linee Guida sulla sicurezza nel procurement ICT

Le **Linee Guida sulla sicurezza nel procurement ICT** raccolgono indicazioni tecnico-amministrative, buone prassi e strumenti operativi (con esempi per agevolarne l'utilizzo), per garantire, all'interno delle procedure per l'approvvigionamento di beni e servizi informatici delle pubbliche amministrazioni, la rispondenza ad adeguati livelli di sicurezza.

Le linee guida hanno la finalità di:

- illustrare in maniera semplice e immediatamente fruibile la problematica della sicurezza nel procurement ICT;
- mettere a sistema (tramite opportuni glossari e

classificazioni), formalizzare definizioni e concetti legati alla sicurezza nel procurement ICT, rendendoli coerenti con la norma e con il contesto della PA;
- presentare buone prassi, soluzioni già in uso, misure semplici da adottare (strumenti operativi, esempi pratici, riferimenti puntuali), per verificare il livello di sicurezza degli attuali processi di acquisizione ed eventualmente per alzare tale livello senza per questo aumentare in modo eccessivo la complessità dei processi e l'impegno necessario a condurli.

Le Linee guida sono frutto del tavolo di lavoro promosso dal **Nucleo per la Sicurezza Cibernetica** (NSC) del Dipartimento Informazioni per la Sicurezza (DIS) presso la Presidenza del Consiglio dei Ministri, che ne ha approvato la stesura. Al documento hanno contribuito, oltre al DIS, il Dipartimento della Protezione Civile, il MAE, il MEF, il MiSE, AgID, Consip, i Ministeri dell'Interno, della Giustizia e della Difesa.

Come partecipare alla consultazione

La consultazione pubblica di entrambe le Linee guida è attiva dal **14 maggio** al **13 giugno 2019**.

Le linee guida sono pubblicate su Docs Italia ed è possibile commentarle su Forum Italia.

Consultazione sulle **Linee Guida sulla sicurezza nel procurement ICT**

Consultazione sulle Linee guida per lo sviluppo e la definizione del modello nazionale di riferimento per i CERT regionali

Per saperne di più: cyber
Cybersecurity nella PA, in consultazione pubblica le linee

guida per i Cert regionali

Spyware tra interferenze illecite ed esigenze di sicurezza informatica

1. **Le intercettazioni nel codice**
2. **Le sanzioni previste dal legislatore**
3. ***Lawful Interception*: il concetto di "*prestazione obbligatoria per fini di giustizia*" e l'evoluzione delle spie telefoniche**
4. **Gli *spyware* come strumento di intercettazione**
5. **Il caso EXODUS**
6. **E' possibile difendersi dagli *spyware*?**

Le intercettazioni nel codice

In un contesto giuridico la definizione di intercettazione è offerta dalla suprema corte di Cassazione nelle linee interpretative della giurisprudenza e della dottrina in materia di intercettazioni[1], ove l'istituto va inteso come "*atto d'indagine mediante il quale, quando è indispensabile ai fini investigativi e ricorrano indizi in ordine alla sussistenza di reati a particolare allarme sociale, viene eseguita la captazione di comunicazioni o conversazioni riservate mediante l'ausilio di mezzi meccanici ed elettronici*".

Uno strumento di ricerca della prova o di prevenzione che,

nell'ordinamento interno, trova compendio negli art. 266 e 266 bis cpp laddove si tratti di intercettazioni giudiziarie, ex art. 226 att. cpp nel caso di intercettazioni preventive ed, ancora, di captazioni in materia di misure di prevenzione ex art. 78 del Decreto legislativo 06.09.2011 n. 159 e di quelle previste per agevolare le prerogative di *intelligence* riconosciute agli agenti delle due Agenzie di Informazione AISI ed AISE, ai sensi dell'art. 12 della L. 133 del 2013, che consentono la possibilità di procedere ad intercettazioni ed all'acquisizione di dati "*quando siano ritenute indispensabili per l'espletamento delle attività demandate dagli articoli 6 e 7 della legge 3 agosto 2007, n. 124".*

Le sanzioni previste dal legislatore

Fuori da questo scenario il legislatore ha disciplinato, in modo severo, ogni abuso all'uso fraudolento di intercettazioni ed alle illecite interferenze nella vita privata, sanzionando, tra l'altro:

1. chi si procura indebitamente[2], mediante l'uso di riprese visive o sonore, notizie attinenti alla vita privata;
2. chi accede abusivamente ad un sistema informatico o telematico;[3]
3. chi prende conoscenza, in modo fraudolento di comunicazioni o conversazioni (*telefoniche o telegrafiche*) comunque a lui non dirette, ovvero le interrompe o le impedisce[4];
4. chi installa apparecchiature tecniche[5], fuori dai casi previsti dalla legge, al fine di intercettare comunicazioni e conversazioni; chi falsifica, altera o sopprime il contenuto di conversazioni[6].
5. chi detiene diffonde abusivamente codici di accesso a sistemi informatici o telematici.[7]

6. chi diffonde apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico[8];
7. chi diffonde riprese e registrazioni fraudolente[9].

Lawful Interception: il concetto di "*prestazione obbligatoria per fini di giustizia*" e l'evoluzione delle spie telefoniche

In un contesto comunitario, il 17 gennaio 1995, il Consiglio Europeo aveva adottato una risoluzione rivolta a prevenire e contrastare il terrorismo e la criminalità all'interno degli stati membri, prevedendo l'obbligatorietà, a carico dei c.d. "*gestori telefonici*", di predisposizione di un sistema di *gateways* sulle dorsali parametriche di comunicazione.

Soltanto otto anni dopo, quando il legislatore riformò il vecchio *Testo Unico delle disposizioni legislative in materia postale, di bancoposta e di telecomunicazioni* risalente al 1973, con l'introduzione del "*CODICE DELLE COMUNICAZIONI ELETTRONICHE*", nel diritto interno è stato introdotto il concetto di diritto comunitario c.d. "*prestazione obbligatoria per fini di Giustizia*" da parte dei gestori telefonici.

Sta di fatto che, da quelle due previsioni del 1995 e del 2003, è rimasta irrisolta, ad oggi, l'individuazione, *de facto*, dei gestori telefonici che non sono oggi inquadrabili in quei colossi social media che forniscono applicazioni di messaggistica internet e di (video) comunicazione VoIP.

Una logica isterica vede *brand* internazionali come TIM, Vodafone, o Wind-H3G, -giusto per citate i marchi più noti in

Italia – vincolati alla richiamata risoluzione in materia di "*prestazione obbligatoria*", a dispetto delle tante "*App*" a portata di taschino che utilizzano la connessione internet di un "gestore" al fine di consentire all'utente di "*chattare*" e videochiamare sui protocolli web (da **WhatsApp**, a **Telegram**, **Viber**, **Skype**, **Messenger** e centinaia di altri applicativi *socialmedia*), a cui vanno ad aggiungersi quelle aziende costruttrici di *device* di alta fascia, che sono in grado di sfruttare internet ed una connessione *wi-fi,* attraverso una piattaforma proprietaria di comunicazione (come ***iMessage*** e ***FaceTime*** per le piattaforme *iOS*, ed in precedenza le *chat pin to pin* ed i ***BlackBerry*** *Message (BBM)*, oggetto peraltro di diffuso interesse della giurisprudenza di legittimità)[10].

In un contesto sovranazionale e geopolitico, l'amministrazione di sistema delle *chat social media*, o dei *brand* costruttori di *devices*, è stata al centro di complesse *querelle* governative, come accaduto, ad esempio, oltre Oceano, per l'accesso, da parte del *Federal Bureau of Investigation* al contenuto di dispositivi **Apple** protetti da crittatura anti-intrusione con autodistruzione, o al fine di accedere ai server di WhatsApp, fino al recente arresto di **Meng Wanzhou**, figlia del magnate di **Huawei** accusata da Washington di "operare per minare gli interessi della sicurezza nazionale degli Stati Uniti".

Fuori dal coro l'atteggiamento collaborativo del primo vettore VoIP, **Skype**, che già nel 2011, con il passaggio a *Microsoft*, aveva messo a disposizione delle autorità governative statunitensi il brevetto "*Legal Intercept*" con*patent application* n. 20110153809, così da consentire l'installazione, in modalità nascosta, di alcuni "*agenti di registrazione*" sia sul computer del *target* oggetto di monitoraggio istituzionale, così da bypassare gli algoritmi proprietari *iLBC (Internet Low Bitrate Codec)* e *SILK (Super Wideband Audio Codec).*

Ecco, allora, l'evoluzione dei *malicious software* – originariamente inoculati per ragioni commerciali non

ortodosse – in insidiosi *spyware* di intercettazione – nel contesto giuridico denominati captatori informatici o *software* di intrusione informatica – per esigenze di captazione (sia essa legale o clandestina) di quegli sbarramenti di flussi telematici incanalati su sistemi di comunicazione sicura "lucchettati" con l'*HyperText Transfer Protocol over Secure Socket Layer* (**HTTPS**), o intellegibili solo tra gli utenti interessati con protocolli proprietari di cifratura o, ancora, protetti da tecnologie di crittografia *end to end* o *peer to peer*, (come i tanti applicativi chat social media di cui è stato fatto cenno) oggi non intercettabili dalla maggior parte dei sistemi tradizionali di intercettazione istituzionale.

La *ratio* dei "*trojan horses*" di intercettazione è quella di insinuarsi – con espedienti di *root o di jailbreak* – nel *device* acquisendone l'amministrazione di sistema per logiche di spionaggio.

In questo contesto, le tecnologie di intercettazione tattica, classificate dalla Comunità Europea come tecnologie "*dual use*" sono state disciplinate dal **Regolamento CE 1334/2000**, sulcontrollo delle esportazioni di prodotti e tecnologie *dual use*, recepito in Italia con l'adozione del **D.Lgs. 96/2003,** fino all'introduzione comunitaria del concetto giuridico di "***software di intrusione***", compendiato nel **Regolamento UE 1382/2014** ed ulteriormente disciplinato dal recente **Regolamento UE 1996/2016,** in tema di esportazione di prodotti "***dual use***", con la previsione, in caso di infrazione, di sanzioni penali di particolare fermezza.

Gli *spyware* come strumento di intercettazione

Nelle intercettazioni a fini giudiziari gli *spyware,* o captatori informatici, ricoprono un ruolo sempre più rilevante. I metodi di intercettazione tradizionali si sono rivelati inefficaci poiché i siti *web* e i servizi di

messaggistica utilizzano metodi crittografici, rendendo in questo modo le comunicazioni e i dati in transito indecifrabili; al contrario, gli *spyware* permettono di collezionare i dati alla fonte, ossia, prima di essere cifrati e trasmessi.

Per spyware o captatore informatico si intende un software, spesso sotto forma di *virus trojan*, in grado di espletare diverse funzioni utili in sede di indagini. A differenza dei *virus* e dei *worm*, gli *spyware* non sono in grado di diffondersi autonomamente, ma richiedono l'intervento dell'utente per essere installati. In questo senso sono dunque simili ai *trojan.* Il termine *spyware*, in un senso più ampio, è solitamente usato per definire un'ampia gamma di *malware*, ossia *software* maligni, dalle funzioni più diverse, quali, ad esempio, l'invio di pubblicità non richiesta (*spam*), la modifica della pagina iniziale o della lista dei Preferiti del *browser*, oppure attività illegali quali la re-direzione su falsi siti di *e-commerce (phishing).*

Molti programmi offerti "gratuitamente" su Internet celano in realtà un *malware*: il *software* è apparentemente gratuito, il prezzo da pagare è un'invasione della *privacy* dell'utente, quasi sempre inconsapevole. Spesso, la stessa applicazione che promette di liberare dagli *spyware* è essa stessa uno *spyware* o ha in realtà installato *spyware*.

Tali *malware*, quindi, si celano spesso, all'interno di altri programmi apparentemente innocui e vanno a infettare il *device target*.[11] Il captatore informatico non viene individuato dai sistemi antivirus dei *device* ove viene allocato, poiché utilizza delle tecniche di mascheramento in grado di eludere i sistemi di rilevamento. I captatori vengono iniettati sfruttando una vulnerabilità all'interno del sistema operativo target non nota nemmeno agli sviluppatori del programma, definita comunemente "*0-day*" (in quanto il programmatore del codice vittima dell'attacco ha zero giorni per poter effettuare la correzione dopo che questo viene attaccato

sfruttando una sua vulnerabilità intrinseca). Talvolta, uno *spyware* può essere installato su un *device* di un inconsapevole utente sfruttando le usuali tecniche di ingegneria sociale, che utilizzano metodi di comunicazione e di persuasione allo scopo di ottenere o compromettere informazioni personali, tramite un vero e proprio studio di ogni soggetto da intercettare.

Alcuni *spyware* vengono eseguiti solo nel momento in cui si utilizza l'applicazione di cui fanno parte e con cui sono stati installati e, dunque, la loro esecuzione cessa nel momento in cui viene chiuso il detto programma. Molti *spyware* hanno, invece, un comportamento più invasivo poiché modificano il sistema operativo del computer ospite in modo da essere eseguiti automaticamente ad ogni avvio. In certe circostanze, l'installazione di *spyware* viene eseguita in maniera ancora più subdola, attraverso pagine Web realizzate appositamente per sfruttare le vulnerabilità dei *browser* o dei loro *plug-in*. Si parla, in questo caso, di *drive by download* (o installazione tramite *exploit*).

Il captatore viene generalmente inoculato con diverse modalità:

- mediante posta elettronica: il *malware* appare come un allegato apparentemente innocuo di posta elettronica;
- mediante web: il *virus* è trasmesso tramite un download effettuato dall'utente da una pagina web;
- mediante trasferimento fisico tramite CD-ROM o un'unità USB da collegare all'apparecchio da infettare;
- mediante infezione dall'esterno attraverso connessione dal *provider* di telecomunicazioni, falsi *update* o siti civetta, oppure tramite IMSI Catcher, anche portatili, che permettono alle forze dell'ordine di portare attacchi di tipo "*man-in-the-middle*" (MTM). Per ragioni di opportunità riguardo le procedure di attacco "istituzionali", si omettono ulteriori dettagli concernenti le tecniche di inoculazione, il cui stato

dell’arte si trova in continua evoluzione per via delle “contromisure” di sovente utilizzate dai *target* per aggirare infezioni.

Una volta inoculato all’interno del sistema, il captatore può svolgere diverse attività e funzioni, tra le quali:

- intercettare chiamate vocali, *chat*, SMS, messaggi istantanei, e-mail;
- catturare immagini dallo schermo del dispositivo;
- acquisire la cronologia telefonica e la lista dei contatti;
- intercettare ciò che viene digitato sulla tastiera del *device*;
- visualizzare la cronologia delle ricerche web e “catturare” le schermate visualizzate sul dispositivo;
- registrare le telefonate effettuate anche mediante applicazioni o programmi (per es. Skype);
- effettuare *download* e *upload* di *file* sul dispositivo stesso;
- realizzare intercettazioni di tipo ambientale con attivazione del microfono;
- mettere in funzione la foto-videocamera di telefoni o computer per vedere i volti delle persone vicine;
- sfruttare i sistemi GPS per geolocalizzare i soggetti sorvegliati;
- svolgere funzioni di *key logger*;
- entrare nella rete domestica dell’utente, attraverso la password del Wi-Fi, e fare ulteriori intercettazioni.

Il caso EXODUS

È evidente la portata rivoluzionaria di questi *software* al fine di effettuare intercettazioni giudiziarie (e, purtroppo, anche di spionaggio illegale). Gli *spyware* sono la risposta allo sviluppo tecnologico, ma sono strumenti talmente invasivi e pericolosi che sollevano dubbi sulla loro affidabilità e la

conciliazione con i nostri diritti umani e costituzionali. Ne è un esempio proprio il recente caso *Exodus*.

Lo *spyware Exodus*, programmato dalla società calabrese eSurv, è un *software* pensato per intercettazioni di Stato, avente come fine principale quello di raccogliere informazioni sull'utente del *device* infetto. Tale *malware* è stato diffuso per errore tramite una ventina di *app,* tutte italiane e in lingua italiana, regolarmente caricate sul *Play Store* di *Google*, i cui filtri non hanno rilevato alcuna minaccia per l'utente. In questo modo lo *spyware* avrebbe intercettato un migliaio di persone che lo hanno scaricato, in quanto contenuto in applicazioni ottenibili gratuitamente. Così, un *software* pensato per spiare legalmente criminali ha intercettato anche più di mille cittadini normali per un presunto errore di programmazione. L'inchiesta è stata condotta dalla società *no profit Security Without Borders* in collaborazione con la rivista *Motherboard.*

Exodus, la cui architettura informatica è rivolta ad intercettare contenuti criminali, è in grado di effettuare diverse operazioni sul telefono della vittima. È dotato di ampie capacità di raccolta e di intercettazione: può, ad esempio, registrare le telefonate e i suoni ambientali (attivando il microfono del telefono), scattare foto con la fotocamera, fare *screenshot*, estrarre informazioni sulle immagini della Galleria, così come copiare gli sms e i numeri di telefono in rubrica, recuperare i file scambiati con *WhatsApp,* conoscere la *password* della rete Wi-Fi a cui si è connessi, acquisire la lista di applicazioni installate e la cronologia di navigazione, leggere la posizione attraverso il GPS, etc.
Le *cyber* intercettazioni di Stato prevedono che, dopo l'autorizzazione del giudice, l'intercettato venga indotto a scaricare lo *spyware*. Per esempio, inviando all'indagato, tramite un operatore *fake* un sms per scaricare l'*app* contenente lo *spyware*, con la promessa di uno sconto, o

utilizzando altre tecniche di ingegneria sociale per indurre al *download*.

Uno *spyware* può essere nascosto anche in un aggiornamento del *firmware* del cellulare: il caso più noto risale al 2009, ed è noto con la sigla *INTERCEPTOR SS8*; allorquando il colosso delle telecomunicazioni ETISALAT (*Emirates Telecommunications Corporation*) aveva inviato un messaggio ai suoi utenti, raccomandando loro di installare un aggiornamento che avrebbe potuto migliorare le prestazioni del 3G sulla piattaforma *Black Berry*[12].

Il *software*, uno *spyware* sviluppato dalla società Californiana specializzata in sorveglianza elettronica SS8, sarebbe stato, a quanto sembra, utilizzato per monitorare gli utenti connessi su ETISALAT [13].

In generale, lo *spyware* permette, a chiunque lo controlli, di gestire a distanza il cellulare dell'utente; il controllore, però, potrebbe essere – anche se indirettamente – la società noleggiatrice che, per conto delle forze dell'ordine ha sviluppato il *software*.

Si tratta, ad onor del vero, una criticità di non poco conto se si considera che molti captatori informatici vengono oggi importati da aziende del settore che acquisiscono il *brand* dal costruttore ma non, anche, i complessivi privilegi di amministratore con le relative chiavi *software*.

Un "pasticcio" che il legislatore ha solo in parte disciplinato, in un'ottica comunitaria con un serie di direttive sulle tecnologie *dual use* di rilevanza strategica[14]; da una focale interna con le novelle introdotte al codice di procedura penale in materia di "captazione informatica", ove sono disciplinate funzioni e caratteristiche dei *software spia**[15]***.

Tornando a *Exodus*, per un errore nel codice, questo *software* ha intercettato in modo indiscriminato qualsiasi utente che

avesse precedentemente scaricato una delle *app*, presenti liberamente sullo *store* di Google, contenente il suddetto *spyware*. La causa che sembra aver scatenato tale problema è stata il mancato funzionamento del filtro per limitare l'intercettazione solo ai cellulari degli indagati (identificabili dal *trojan* tramite il codice IMEI del dispositivo).

La maggior parte delle app in questione si presentava come strumento per migliorare le prestazioni del cellulare. 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. Secondo Google una di queste applicazioni malevole ha raccolto oltre 350 installazioni, mentre altre varianti hanno raccolto poche decine ciascuna[16].

Tutte le infezioni sono state localizzate in Italia. Il virus gira almeno dal 2016, quindi è possibile che ci siano altre applicazioni infette che ancora devono essere scoperte. È preoccupante che alcune delle modifiche effettuate dallo *spyware* potrebbero esporre i dispositivi infetti ad ulteriori compromissioni o a manomissioni dei dati. Secondo *Security Without Borders* le responsabilità delle società sono più gravi rispetto ad un semplice errore di programmazione[17].

È sicuramente interessante capire il funzionamento del *virus Exodus*. L'infezione da *Exodus* ha inizio scaricando e installando una delle app infette. Il virus si compone di due *stage*, denominati "*Exodus 1*" ed "*Exodus 2*". Il primo ha il compito di leggere il codice IMEI del cellulare e comunicarlo al *server* di *Command & Control****[18]***.

Security Without Borders ha scoperto che, anche se l'IMEI inviato è quello di un cellulare nuovo usa e getta, attivato solo per scopi di test, *Exodus* si attiva lo stesso, scaricando il secondo pacchetto *Exodus 2* contenente il virus vero e proprio, che inizia a "tracciare" il comportamento

dell'utente. *Exodus*, volutamente o per errata programmazione, lascia diverse porte aperte e rende vulnerabile lo *smartphone* a chiunque sia connesso alla stessa rete Wi-Fi e, forse, persino alla stessa cella dell'operatore di telefonia mobile.

Supponiamo che un programma non attendibile (ad esempio *drive-by download* o qualsiasi programma *spyware*) venga scaricato da un ambiente non affidabile (ad esempio Internet) e venga installato sul sistema con conseguente violazione dell'integrità del sistema.[19] La violazione dell'integrità porta all'*escalation* dei diritti di accesso, il che si traduce in compromessi, in termini di *availability* (ad es. lo *spyware* consuma la CPU e le risorse di rete) e *confidentiality* (ad es. *cookie*, la cronologia di navigazione viene raccolta e inviata ad una parte non autorizzata). È chiaramente necessario un meccanismo che specifichi il flusso di informazioni non sicure (ad esempio programmi sospetti che accedono a file sensibili) e che applichi le politiche di sicurezza (ad esempio la rimozione del programma *spyware)* all'interno dell'*host client*.

Anche componenti benigne possono generare attività sensibili, ma la profondità e la frequenza di queste attività consentono di effettuare una distinzione dai componenti dello *spyware*. Un eseguibile benigno, ad esempio, non si nasconderebbe mai o non si ripristinerebbe da solo quando un utente tenta di disinstallarlo o rimuoverlo.

Fig.1. Un modello di invasioni di *spyware* comuni. Le frecce rappresentano un flusso di informazioni non sicuro che causa alcune violazioni di sicurezza.
Perché un *virus* creato ad arte per eseguire approfondite intercettazioni ambientali ha "colpito" anche utenti normali? Secondo l'ipotesi più diffusa, *Exodus* sarebbe stato caricato su *Play Store* affinché lo si potesse testare prima di utilizzarlo in indagini ufficiali[20].

Secondo il Garante della *privacy* Antonello Soro: "*È un fatto gravissimo. La notizia dell'avvenuta intercettazione di centinaia di cittadini del tutto estranei ad indagini giudiziarie, per un mero errore nel funzionamento di un captatore informatico utilizzato a fini investigativi, desta grande preoccupazione e sarà oggetto dei dovuti approfondimenti, anche da parte del Garante, per le proprie competenze. La vicenda presenta contorni ancora assai incerti ed è indispensabile chiarirne l'esatta dinamica*"[21].

E' possibile difendersi dagli SPYWARE?

Sicuramente, è necessario apportare dei miglioramenti alla normativa vigente al fine di obbligare queste società (come eSurv) ad adottare misure tecniche di sicurezza più stringenti, per esempio obbligando a usare cifratura con chiavi solo in possesso degli operatori giudiziari.

È importante precisare che i *malware* incidono sul funzionamento e sulle prestazioni del *device* su cui sono installati. All'attività principale degli *spyware,* ossia quella di raccogliere informazioni, si affiancano degli effetti collaterali, come la riduzione della velocità percepita dall'utente, l'occupazione di cicli di CPU e di spazio nella memoria RAM, la difficoltà di connettersi ad Internet, la presenza di tentativi di connessione non richiesti dall'utente, fino all'instabilità, a forme di *crash* o al blocco del sistema.

Ovviamente, nessuno *spyware* ha lo scopo di rendere inutilizzabile il sistema su cui è installato, in quanto esso deve essere funzionante per poter consentire la raccolta delle informazioni. I sistemi non protetti possono accumulare centinaia di *spyware*. L'utente, il più delle volte, attribuisce tali malfunzionamenti a difetti del sistema operativo od a problemi *hardware* o a *virus*, e ricorre quindi

ad azioni radicali come la formattazione e la re-installazione del sistema.

L'utilizzo di un *antivirus*, purtroppo, può non essere sufficiente a proteggere dagli *spyware*, dato che essi non sono *virus o worm*. Esistono invece specifici programmi *antispyware* realizzati proprio per rilevare e cancellare gli *spyware* dal sistema. Tuttavia, la rimozione di un componente *spyware* potrebbe comportare il malfunzionamento del *software* di cui esso faceva parte, e inoltre non tutti gli *spyware* vengono sempre riconosciuti o rimossi da *antivirus* e *antispyware*.

La strategia più efficace per difendersi dagli *spyware* è diffidare da qualsiasi *software* offerto gratuitamente da siti che non siano quelli ufficiali ed evitare di seguire i *link* contenuti nei messaggi di spam ricevuti nella casella di posta elettronica. È fondamentale anche aggiornare frequentemente il proprio sistema operativo con le *patch* rilasciate dal produttore al fine di prevenire l'installazione di *spyware* che sfruttano le vulnerabilità del sistema.

Non esiste ad oggi un modo per difendersi pienamente dagli *spyware*, ma esistono comportamenti e tecniche per limitarne almeno il raggio d'azione.

È legittimo, dunque, nutrire preoccupazioni per le accresciute potenzialità scrutatrici ed acquisitive dei virus informatici, suscettibili di ledere riservatezza, dignità e libertà delle persone, ma, dato lo stato delle comunicazioni sociali, l'utilizzo di tecniche investigative così invasive rappresenta un adeguamento del sistema processuale alle nuove metodiche comunicative ed è ormai una necessità intrinseca per svolgere l'attività di indagine in maniera efficace, ovviamente nel caso in cui si agisca per l'accertamento di determinati reati.

Senza tali tecniche, sarebbe impossibile ottenere validi risultati dalle indagini tradizionali, stante la sempre più frequente criptazione delle comunicazioni. Solo questi

strumenti permettono di penetrare canali criminali di comunicazione o di scambio di informazioni utilizzati per la commissione di gravissimi reati contro le persone. Occorre, pertanto, colmare il vuoto normativo a vantaggio dei cittadini e degli inquirenti con una compensazione che, nel salvaguardare i principi fissati, da un parte, dall'art. 8 CEDU in materia di privacy dell'individuo, trovi bilanciamento in quelle necessità di tutela e di *salus rei publicae****[22]***, fissato dall'art. 52 della nostra Carta costituzionale.

---

[1] Suprema Corte di Cassazione, Uff. del Massimario, Serv. Penale Rel. N. 55/2005 Orientamenti sulle linee interpretative della Giurisprudenza e della dottrina in materia di intercettazioni, p. 5: *"Gravi indizi di reato (art. 267 comma 1 c.p.p.). Punto di partenza della analisi è che i gravi indizi che, ai sensi dell'art. 267, comma 1, cod. proc. pen. costituiscono presupposto per il ricorso alle intercettazioni, attengono all'esistenza del reato e non alla colpevolezza di un determinato soggetto; per procedere ad intercettazione non è pertanto necessario che i detti indizi siano a carico dei soggetti le cui comunicazioni debbano essere, a fine di indagine, intercettate (Sez. VI, 18 giugno 1999, n. 9428, Patricelli F., rv 214127; sez. V, 7 febbraio 2003, n. 38413, Alvaro e altri, rv 227413). Ancor meglio precisa sez. V, 8 ottobre 2003, n. 41131, Liscai, rv 227053, che i presupposti della intercettazione sono la sua indispensabilità ai fini delle indagini e la sussistenza dei gravi indizi di reato. Tale secondo requisito va inteso non in senso probatorio (ossia come valutazione del fondamento dell'accusa), ma come vaglio di particolare serietà delle ipotesi delittuose configurate, che non devono risultare meramente ipotetiche, con la conseguenza che è da ritenere legittimo il decreto di intercettazione telefonica disposta nei confronti di un soggetto che non sia iscritto nel registro degli indagati. Da tale principio si è fatto discendere il corollario che "la*

mancata individuazione dell'autore dell'illecito in relazione al quale è disposta la intercettazione influisce sulla utilizzabilità dei suoi effetti nello stesso procedimento ai fini di prova di condotte criminose collegate". (Sez. I, 3 dicembre 2003, n. 16779, Prota ed altro, rv 227914). Si registra un contrasto in giurisprudenza sulla possibilità di utilizzare, quale indizio di reato ai fini della autorizzazione alla intercettazione, le dichiarazioni spontanee dell'indagato rese a norma dell'art. 350 c.p.p. non verbalizzate nelle forme dell'art. 357 ma annotate sommariamente in forma libera. Da un lato, sez. VI, 22 gennaio 2004, n. 14980, Picano, rv 229398, ha rilevato che queste possono essere utilizzate erga alios quali indizi nella fase delle indagini preliminari ai fini dell'autorizzazione dell'intercettazione di conversazioni o comunicazioni telefoniche nell'ambito di un procedimento per delitti di criminalità organizzata, non ricorrendo alcuna ipotesi di inutilizzabilità generale di cui all'art. 191 dello stesso codice ovvero di inutilizzabilità specifica. Dall'altro, per sez. I, 12 ottobre 1994, n. 4480, Savignano, rv. 200226, la mancata verbalizzazione, da parte della polizia giudiziaria, di atti che, ai sensi dell'art. 357, comma secondo, cod. proc. pen., dovrebbero essere verbalizzati comporta che tali atti, in quanto privi di documentazione, siano da considerare inesistenti e, come tali, indipendentemente da ogni riferimento alle categorie della nullità e della inutilizzabilità, inidonei ad essere assunti a base anche della semplice adozione di misure cautelari".

[2] Art. 615 bis c.p. *Interferenze illecite nella vita privata:* «Chiunque mediante l'uso di strumenti di ripresa visiva o sonora, si procura indebitamente notizie o immagini attinenti alla vita privata svolgentesi nei luoghi indicati nell'articolo 614, è punito con la reclusione da sei mesi a quattro anni.

Alla stessa pena soggiace, salvo che il fatto costituisca più

grave reato, chi rivela o diffonde, mediante qualsiasi mezzo di informazione al pubblico, le notizie o le immagini ottenute nei modi indicati nella prima parte di questo articolo. I delitti sono punibili a querela della persona offesa; tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o servizio, o da chi esercita anche abusivamente la professione di investigatore privato».

[3] Art. 15 ter c.p. *Accesso abusivo ad un sistema informatico o telematico*. " Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni. La pena è della reclusione da uno a cinque anni: 1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.
Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni.Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio.

[4] Art. 617 c.p. *Cognizione interruzione o impedimento illeciti di comunicazioni o conversazioni telegrafiche o telefoniche:* «Chiunque fraudolentemente, prende cognizione di una comunicazione o di una conversazione, telefoniche o telegrafiche, tra altre persone o comunque a lui non dirette, ovvero le interrompe o le impedisce è punito con la reclusione da sei mesi a quattro anni. Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni o delle conversazioni indicate nella prima parte di questo articolo. I delitti sono punibili a querela della persona offesa; tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso in danno di un pubblico ufficiale o di un incaricato di un pubblico servizio nell'esercizio o a causa delle funzioni o del servizio, ovvero da un pubblico ufficiale o da un incaricato di un pubblico servizio con abuso dei poteri o con violazione dei doveri inerenti alla funzione o servizio, o da chi esercita anche abusivamente la professione di investigatore privato».

Art. 617 quater c.p. *Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche*: «Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni. Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma. I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa. Tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso: 1) in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità; 2) da un pubblico

ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema; 3) da chi esercita anche abusivamente la professione di investigatore privato».

[5] Art. 617 bis c.p. *Installazione di apparecchiature atte ad intercettare od impedire comunicazioni o conversazioni telegrafiche o telefoniche:* «Chiunque fuori dei casi consentiti dalla legge, installa apparati, strumenti, parti di apparati o di strumenti al fine di intercettare od impedire comunicazioni o conversazioni telegrafiche o telefoniche tra altre persone è punito con la reclusione da uno a quattro anni. La pena è della reclusione da uno a cinque anni se il fatto è commesso in danno di un pubblico ufficiale nell'esercizio o a causa delle sue funzioni ovvero da un pubblico ufficiale o da un incaricato di un pubblico servizio con abuso dei poteri o con violazione dei doveri inerenti alla funzione o servizio o da chi esercita anche abusivamente la professione di investigatore privato».

Art. 617-quinquies c.p. Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche: «Chiunque, fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi, è punito con la reclusione da uno a quattro anni. La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617-quater».

[6] Art. 617 ter. c.p. *Falsificazione, alterazione o soppressione del contenuto di comunicazioni o conversazioni telegrafiche o telefoniche*. «Chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, forma falsamente, in tutto o in parte, il testo di una comunicazione o di una conversazione telegrafica o telefonica ovvero altera o sopprime in tutto o in parte il contenuto di

una comunicazione o di una conversazione telegrafica o telefonica vera, anche solo occasionalmente intercettata, è punito, qualora ne faccia uso o lasci che altri ne faccia uso, con la reclusione da uno a quattro anni. La pena è della reclusione da uno a cinque anni se il fatto è commesso in danno di un pubblico ufficiale nell'esercizio o a causa delle sue funzioni ovvero da un pubblico ufficiale o da un incaricato di un pubblico servizio con abuso dei poteri o con violazione dei doveri inerenti alla funzione o servizio o da chi esercita anche abusivamente la professione di investigatore privato».

[7] Art. 615 quater. *Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici.* "Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino ad un anno e con la multa sino a euro 5.164. La pena è della reclusione da uno a due anni e della multa da euro 5.164 a euro 10.329 se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'articolo 617-quater.

[8] Art. 615 quinquies. *Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico*. "Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino

a euro 10.329”.

[9] Art. 617-*septies* c.p. *Diffusione di riprese e registrazioni fraudolente*. “Chiunque, al fine di recare danno all’altrui reputazione o immagine, diffonde con qualsiasi mezzo riprese audio o video, compiute fraudolentemente, di conversazioni, anche telefoniche o telematiche, svolte in sua presenza o con la sua partecipazione, è punito con la reclusione fino a quattro anni. La punibilità è esclusa se la diffusione delle riprese o delle registrazioni deriva in via diretta ed immediata dalla loro utilizzazione in un procedimento amministrativo o giudiziario o per l’esercizio del diritto di difesa o del diritto di cronaca”.

[10] “*In tema di intercettazioni telefoniche, l’acquisizione della messaggistica, scambiata mediante sistema BlackBerry, non necessita di rogatoria internazionale quando le comunicazioni sono avvenute in Italia, a nulla rilevando che per ‘decriptare i dati indentificativi associati ai codici PIN occorra ricorrere alla collaborazione del produttore dei sistemi operativo avente sede all’estero’’* (*Ex plurimis,* Cassazione n. 52925/2016; Cassazione n. 16670/2016).

[11] Barbara Indovina, *“I captatori informatici: una riforma troppo contenuta per uno strumento investigativo così pervasivo”,* Rivista di diritto dei media 2/2018.

[12] www.wired.com, Sheran A. Gunasekera, *Analizzando il SS8 Interceptor Application per il palmare BlackBerry,* ABSTRACT: “[…] Questo documento fornisce informazioni su BlackBerry spyware conosciuto come “Interceptor.” Il software è stato sviluppato dalla società Intercettazione legale SS8 ed è stato distribuito agli abbonati del gestore delle telecomunicazioni degli Emirati Arabi Uniti, Etisalat come un aggiornamento. […] Intorno l’8 luglio 2009, BlackBerry abbonati della base di telecomunicazioni UAE ricevuto Messaggio push WAP avevano richiesto loro di scaricare un aggiornamento. […].

[13] www.blog.armandoleotta.com, *BlackBerry: Update con spyware?,* 28 luglio 2008 by ArMyZ: " […] La piattaforma BlackBerry non è nuova a situazioni in cui si mette in discussione il rispetto della privacy. Questa volta la situazione è un po' diversa e riguardo un aggiornamento software. Spedito come un WAP PUSH MESSAGE, l'aggiornamento in questione istalla un file java sul dispositivo mobile. Tutto normale se questo aggiornamento, spedito agli utenti blackberry sulla rete ETISALAT negli Emirati Arabi, altro non fosse che un'applicazione in grado di intercettare sia mail che sms, spedirne una copia ad un server Etisalat, il tutto all'insaputa dell'ignaro utente che notava solo un degrado della durata della batteria. Pare che proprio questo aspetto abbia insospettito alcuni utenti e sviluppatori che ad un controllo più approfondito si sono ritrovati di fronte a questa sorpresa. L'aggiornamento era così etichettato: "Etisalat network upgrade for BlackBerry service. Please download to ensure continuous service quality." Il file JAR, firmato, faceva riferimento ad una applicazione nel percorso /com/ss8/interceptor/app […].

[14] M. Di Stefano*, Prodotti e tecnologie dual use, tra UE e giurisprudenza interna: sicurezza degli stati membri Vs esigenze di privacy*, pubblicato dalla rivista di sicurezza informatica ICT Security Magazine, articolo del 6.09.2017.

[15] M. Di Stefano, B. Fiammella, *Intercettazioni: Remotizzazione e diritto di difesa nell'attività investigativa (profili d'intelligence), II edizione con gli aggiornamenti del D.l.vo 216/2017"*, "*Collana Professionale*", ALTALEX, Montecatini Terme (2018).

[16] www.adnkronos.com, *Spyware di Stato, migliaia di italiani intercettati.* Pubblicato da adnkronos il 30. 03. 2019.

[17] A. Longo, *Più di mille italiani intercettati sul cellulare, per errore, da un hacker di Stato.*

[18] https://tecnologia.libero.it, *20 app infette da Exodus vi spiano: quali sono e come cancellarle,* Pubblicato da Libero/Tecnologia, 1. 04. 2019.

[19] Ming-Wei Wu, Student Member, IEEE, Yi-Min Wang, Member, IEEE, Sy-Yen Kuo, Fellow, IEEE, and Yennun Huang, Member, IEEE. *Self-Healing Spyware: Detection, and Remediation.*

[20] https://tecnologia.libero.it, *20 app infette da Exodus vi spiano: quali sono e come cancellarle,* Pubblicato da Libero/Tecnologia, 1. 04. 2019.

[21] A. Longo, *Più di mille italiani intercettati sul cellulare, per errore, da un hacker di Stato.*

[22] M. Di Stefano, *Salus rei publicae e terrorismo moderno: esigenze di prevenzione e contrasto* pubblicato dalla rivista giuridica ALTALEX, articolo dell'18.09.2017.

https://www.key4biz.it/spyware-tra-interferenze-illecite-ed-esigenze-di-sicurezza-informatica/257670/

Cybercrime, truffati oltre 100 venditori Amazon in Uk

Lo scorso anno per oltre 6 mesi, oltre 100 rivenditori (seller) Amazon sono stati vittime di un imponente hack".

Bloomberg conferma che l'azienda di **Jeff Bezos** ha dichiarato di essere stata colpita tra maggio e ottobre 2018, rivelando che hacker non identificati sono stati in grado di sottrarre fondi dai conti di circa 100 commercianti versandoli direttamente sui propri conti correnti.

In pratica non sono stati truffati i clienti, ma i rivenditori, in quanto gli utenti procedevano con gli ordini e i pagamenti, ma gli accrediti confluivano sui conti dei pirati informatici.

Sempre secondo Bloomberg lo stesso è avvenuto per il programma di prestiti che Amazon concede a venditori e startup chiamato **Amazon Capital Services**, che mette a disposizione dei venditori un servizio di prestiti a condizioni particolari.

Amazon, che ha terminato le indagini solo ora, ha scoperto che gli hacker sono riusciti a modificare i dettagli degli account sulle piattaforme di vendita della banca **Barclays** e di **Prepay Technologies**, e che gli account sono stati compromessi dalle tecniche di phishing.

L'azienda americana non ha spiegato come i presunti malfattori siano stati in grado di modificare i profili dei seller.

https://www.key4biz.it/cybercrime-truffati-oltre-100-venditori-amazon-in-uk/257388/

Sicurezza informatica e privacy, entra in gioco l'informatica quantistica con il "qubit"

Nelle ultime ore ha fatto scalpore l'attacco informatico del collettivo LulzSec_ITA, che ha sottratto e diffuso online

oltre 30.000 credenziali di PEC di membri dell'Ordine degli Avvocati di Roma. nomi eccellenti, tra cui il sindaco di Roma, Virginia Raggi.
Un fatto grave, che evidenzia le ancora troppo grandi vulnerabilità delle organizzazioni e allo stesso tempo l'efficacia delle azioni dei cyber criminali, a cui però è possibile porre rimedio.
Nel mondo, secondo Cybersecurity Ventures, dal 2013 ad oggi, sono stati rubati giornalmente 3.809.448 dati personali e sensibili: ogni secondo, in sostanza, vengono sottratti dati da 44 account per mezzo di attacchi informatici.

Questo significa, che password di accesso, numeri di carte di credito e messaggi di chat, sono tutti protetti da complicati algoritmi matematici, che sono alla base dei moderni sistemi di crittografia. Sistemi avanzatissimi, ma ancora non perfetti.
Nello **studio** intitolato "***All-fiber self-compensating polarization encoder for Quantum Key Distribution***",pubblicato dalla rivista *Optics Letters*, il gruppo di ricerca "*QuantumFuture*" del dipartimento di Ingegneria dell'informazione dell'**Università di Padova** ha proposto un nuovo sistema di crittografia basato sullo scambio di "*quantum bit*" (o "***qubit***").

Stiamo parlando di informatica quantistica e il *qubit* è la versione quantistica del bit classico: "*mentre il bit classico può assumere solo due valori distinti, 0 oppure 1, il qubit si può trovare in una "sovrapposizione" quantistica tra i due stati |0> e |1>",* si legge in un articolo pubblicato sul sito dell'ateneo *ilbolive.unipd.it*.
I ricercatori di Padova presentano quella che è definita la "***distribuzione quantistica di chiave***", o in sigla QKD, che permette di "*creare una chiave di cifratura condivisa e sicura tra due utenti*": "*La chiave è creata codificando i qubit nella polarizzazione (la polarizzazione della luce è legata alla direzione di oscillazione del campo elettrico) di singoli*

fotoni scambiati tra essi".

La sicurezza è garantita dalle **leggi della meccanica quantistica**, che assicurano che "*nessun altro utente può avere informazioni sulla chiave. Tali leggi assicurano che non esiste la "fotocopiatrice quantistica" (un qubit non può essere copiato) e che una qualunque misura sul qubit ne altera il suo stato*".
"***Ci si aspetta che la QKD abbia un profondo impatto sulla privacy e sulla sicurezza dei cittadini*** – ha dichiarato nell'articolo **Giuseppe Vallone**, che ha guidato questa ricerca all'interno del gruppo QuantumFuture coordinato dal co-autore **Paolo Villoresi** – *il nostro schema semplifica la generazione di qubit codificati nella polarizzazione dei fotoni. La polarizzazione è in particolare la codifica più adatta alle comunicazioni quantistiche in spazio libero, come da satellite verso Terra o tra i terminali mobili, in quanto non viene perturbata durante la propagazione*".

Il sistema sviluppato dal gruppo di ricerca "*QuantumFuture*", "*per codificare efficientemente e rapidamente i qubit nella polarizzazione dei singoli fotoni*", chiamato **schema POGNAC** (da *Polarisation Sagnac*), permette di avere un dispositivo compatto, completamente in **fibra ottica** e "*autocompensante*": "*è stato realizzato con componenti commerciali, tipicamente usati per le comunicazioni classiche in fibra, permettendo di modulare la polarizzazione più di un miliardo di volte al secondo e al contempo semplificando il setup e riducendo i costi totali del dispositivo. Grazie a questi due fattori chiave – stabilità e alta velocità di modulazione – questo schema risulta ideale per i protocolli di QKD in spazio libero e in fibra*".

https://www.key4biz.it/sicurezza-informatica-e-privacy-entra-in-gioco-linformatica-quantistica-con-il-qubit/257160/

Cyber attack, Vulnerability Assessment & Penetration, il decalogo per prevenire attacchi informatici

È notizia recente l'attacco "multiplo" alle credenziali e ai dati di molte mail **Pec** di noti professionisti contenenti anche dati sensibili.

L'occasione può essere utile per focalizzarci ancora una volta su tema assai sottostimato e cioè la *cybersecurity*.

Abbiamo già detto che la componente umana è uno dei grimaldelli dei sistemi di sicurezza informatica.

Ribadiamo in questa sede l'importanza di una buona formazione del personale e, d'altro canto, è utile osservare come un sistema di prevenzione *tailor-made* sia l'arma più efficace per problemi simili.

1. Anzitutto dovrebbe essere effettuato un *general assessment* sulle vulnerabilità attuali del sistema.
2. Successivamente sarebbe utile implementare le misure di sicurezza del sistema informatico.
3. Infine sarebbe utile proteggersi con una buona polizza assicurativa contro i rischi di intrusione informatica.

Sotto quest'ultimo profilo è utile verificare che la copertura assicurativa e la relativa assistenza siano effettivamente

utili (ad esempio bisognerebbe verificare le definizioni fornite dei vari attacchi informatici, la territorialità della copertura, la durata, le clausole di esclusione ed il massimale).

I. Ad ogni modo potremo così sintetizzare un decalogo per proteggere il nostro sistema informatico:

1. stabilire la qualità e la consistenza del sistema informatico;
2. effettuare una prima analisi del sistema informatico per individuarne eventuali vulnerabilità;
3. stilare un rapporto sulle vulnerabilità del sistema informatico;
4. aggiornare i sistemi operativi e degli applicativi finalizzati alla protezione del sistema informatico e dei dati informatici (quali ad esempio antivirus, firewall e simili);
5. verificare le connessioni in uscita del sistema informatico;
6. configurare un sistema di ripristino (ad esempio il backup);
7. installare un sistema software finalizzati a limitare le conseguenze di un attacco informatico (ad esempio per gestire un ransomware);
8. stilare un protocollo delle misure di sicurezza attuate e loro aggiornamento (ad esempio gestione, aggiornamento delle password) e stilare un protocollo di gestione di attacco informatico e costituzione di un team dedicato;
9. monitoraggio del funzionamento del sistema di protezione;
10. simulazioni di aggressioni con cadenza programmata.

II. Accanto all'implementazione del sistema informatico è utile o addirittura sovrapponibile un sistema di protezione e gestione dei dati personali.

Sul punto osserviamo che già un sistema di trattamento dei

dati conforme alla normativa vigente sarebbe sufficiente a porre in sicurezza il nostro sistema informatico.

Non guasta sul punto applicare lo standard internazionale **ISO 27001.**

Infatti, applicando gli obblighi previsti dal GDPR (oltre al novellato codice) e seguendo le *best practice* ISO 27001 è possibile costruire un sistema integrato di gestione sicura dei dati aziendali.

Sarebbe utile dimostrare particolare sensibilità all'**Audit** con cadenza programmata per identificare le modalità di inosservanza degli obblighi in materia di protezione dei dati personali contenuti nel sistema informatico.

Infine sarebbe utile ipotizzare scenari di ripristino e impatti sul business, creando un sistema di *cyber resilient*.

A questo punto si potrebbe dare origine ad un unico "**ecosistema" di protezione dei dati** sia personali che aziendali capace di sopportare i più comuni attacchi informatici.

Per approfondire

In corso attacco hacker all'Ordine degli Avvocati di Roma (inclusa Virginia Raggi). Password in chiaro e PEC violate

https://www.key4biz.it/cyber-attack-vulnerability-assessment-penetration-il-decalogo-per-prevenire-attacchi-informatici/257107/

Elezioni europee a rischio cyber attacchi, allertati NATO e team pronto intervento UE

Le **elezioni per il rinnovo del Parlamento europeo** si stanno avvicinando (23-26 maggio) e aumentano i timori di **possibili, quanto concreti, attacchi informatici** tesi al sabotaggio delle stesse. Un workshop sull'argomento è stato organizzato a fine aprile dall'Organizzazione del Trattato dell'Atlantico del Nord (**NATO**) e dal Computer Emergency Response Team dell'Unione europea (CERT-EU).

L'incontro ha permesso all'agenzia della NATO per la comunicazione e l'informazione (**NCI**) e la squadra di pronto intervento informatico per le istituzioni, gli organi e le agenzie dell'Unione europea (CERT-EU) di confrontarsi sulle possibili minacce informatiche alla tornata elettorale e sui provvedimenti che necessariamente vanno presi per fronteggiarle al meglio.

"*Come ha affermato il Segretario generale, Jens Stoltenberg, la NATO deve fungere da punto di riferimento per la condivisione delle informazioni, la formazione e l'esperienza*", ha dichiarato **Ian West**, Cyber Security Chief dell'NCI.
"*Attraverso l'accordo con il CERT-EU, la nostra agenzia per la comunicazione e l'informazione può intevenire convocando i suoi partner industriali per discutere potenziali minacce, suggerendo misure per contrastarli ed esplorando nuovi modi di diffondere informazioni utili. Sebbene le Nazioni siano le principali responsabili della sicurezza dei sistemi elettorali, la NATO è pronta a fornire supporto per esaminare il panorama delle minacce, nonché fornire informazioni sui*

processi e le tecniche utili a proteggere eventi di alto profilo".

"*Lo scambio di buone pratiche e la condivisione di informazioni su tali temi sono azioni che rafforzano il nostro partenariato strategico*", ha dichiarato in una nota **Saâd Kadhi**, Responsabile del CERT-EU.
"*Il workshop arriva in un momento fondamentale per le nostre Istituzioni, un mese prima delle elezioni europee, ed è un anche un esempio eccellente del nostro impegno nella cybersecurity e della cooperazione crescente tra i nostri team di cyber difesa*".

Diverse, ovviamente, le indicazioni emerse sui possibili cyber attacchi che potrebbero riguardare l'esercizio di voto nei giorni previsti per le elezioni dei nuovi membri del Parlamento europeo. Si va dallo *spear phishing* agli gli attacchi distribuiti di negazione del servizio (DDoS).

Lo ***spear phishing*** è una truffa tramite comunicazioni elettroniche o email, indirizzata a una persona, un'organizzazione o un'azienda specifica. Sebbene abbia spesso l'obiettivo di sottrarre dati per scopi dannosi, i cybercriminali potrebbero anche voler installare malware sul computer dell'utente preso di mira.
Come spiegano i ricercatori di Kaspersky, con questa tecnica, i cyber criminali agiscono con l'intento di rivendere i dati riservati a governi e aziende private. Essi utilizzano approcci e tecniche di social engineering su misura personalizzando in modo efficace messaggi e siti Web. Di conseguenza, anche gli obiettivi più alti all'interno delle organizzazioni, ad esempio i massimi dirigenti, possono trovarsi ad aprire e-mail ritenute sicure. Un tale errore consente ai cybercriminali di rubare i dati di cui hanno bisogno per attaccare le reti.

In un tipico attacco **DDoS (*Distributed Denial of Service*),** invece, il normale traffico di un server viene interrotto da un sovraccarico di traffico Internet proveniente da sistemi compromessi, come computer o altri dispositivi collegati.
Le risorse di rete, come i server Web, hanno un limite preciso in termini di numero di richieste che sono in grado di soddisfare contemporaneamente. Oltre alla capacità limitata del server di accettare richieste, anche il canale che connette il server a Internet avrà una data larghezza di banda o capacità. Ogni volta che il numero di richieste supera la capacità di qualsiasi componente dell'infrastruttura, molto probabilmente il livello del servizio ne risentirà in uno dei modi seguenti: la risposta alle richieste sarà molto più lenta del normale; alcune, se non tutte, le richieste degli utenti potrebbero essere completamente ignorate.

Il workshop Nato-Cert ha reso evidente la necessità di continuare a insistere sulla formazione e la consapevolezza degli utenti, in particolare per quanto riguarda attacchi come il ***phishing***, che è un approccio molto efficace utilizzato dagli hacker per spingere gli utenti a rivelare informazioni personali, quali password o dati delle carte di credito o dei conti correnti bancari. Tale operazione avviene inviando mail fasulle o indirizzando l'utente su un sito web costruito ad arte per lo scopo.
Dalla valutazione del workshop è emerso, infine, che i funzionari governativi e i loro partner nelle imprese private devono continuare a collaborare e a condividere le informazioni sulle minacce.

> *Elezioni europee a rischio cyber attacchi, allertati NATO e team pronto intervento UE*