Research Shows Twitter Manipulation in Weeks Before EU Elections

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/xC5am0DNJ8I/research-shows-twitter-manipulation-weeks-eu-elections

---

AgID continua a spingere in alto la resilienza della PA agli attacchi cyber

*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**.*

Mentre in molte organizzazioni i Security Manager soffrono per una scarsa consapevolezza del personale sulla gravità delle possibili minacce e, spesso, anche per le indesiderate riduzioni di budget (vedi i miei precedenti articoli sulla "solitudine del security manager"), la Pubblica Amministrazione, locale e centrale, ha a disposizione – tra l'altro in modo totalmente gratuito – team specialistici per accompagnarle nella realizzazione di appositi progetti di sicurezza delle informazioni, finalizzati alla riduzione del rischio.

In questo modo il Dirigente Responsabile della Trasformazione

Digitale può avvalersi di consulenti esperti in risk management, ICT Security, business continuity e crisis management senza intaccare il (spesso già ridotto) budget.

Infatti, sia il Piano Triennale per l'Informatica nella Pubblica Amministrazione 2016-2019 che quello da poco tempo approvato, per il 2019-2021, stanno dando un impulso notevole alla trasformazione digitale in atto e in modo particolare alla sicurezza.

AgID agisce coerentemente con il Piano e le norme vigenti, che «le conferiscono un mandato importante nell'attuazione di iniziative tecniche ed organizzative volte sia a migliorare la consapevolezza della Pubblica Amministrazione nei riguardi della minaccia, sia ad aumentarne le capacità di prevenzione, protezione e risposta agli incidenti». In particolare, le è stato attribuito il compito di «dettare indirizzi, regole tecniche e linee guida in materia di sicurezza informatica e di omogeneità degli standard, di assicurare la qualità tecnica e la sicurezza dei sistemi informativi pubblici e della loro rete di interconnessione e di monitorare i piani ICT delle amministrazioni pubbliche».

AgID persegue questo mandato sia direttamente, sia mediante il **CERT-PA.**

Per completezza informativa, cito che il Rapporto "Italian Cyber Security Report 2014" aveva rilevato la mancanza nelle pubbliche amministrazioni della consapevolezza sulla minaccia, e l'assenza di strutture organizzative locali in grado di operare efficacemente un'attività di preparazione e risposta agli incidenti. Sulla base di tali rilevazioni, AGID ha avviato un'azione di *awareness*, condotta dal CERT-PA, e la pubblicazione di documenti di indirizzo ed operativi (linee guida, regole tecniche), finalizzati ad accrescere la

consapevolezza e la capacità di difesa delle Amministrazioni interessate.

Mi si consenta di suggerire – anche a chi non appartiene o non collabora con la PA – di consultare i documenti messi a disposizione sul sito istituzionale (www.agid.gov.it), in quanto utili, ben fatti, sia dal punto di vista tecnico, sia di coerenza con la normativa vigente e le esigenze di realtà che trattano dati riservati e sensibili (ad esempio: le linee guida per lo sviluppo sicuro, il cloud, il procurement, le misure minime – standard – avanzate di sicurezza da adottare, design e sviluppo sicuro, ecc.).

In chiusura, segnalo che il primo passo, del programma attuale di "accompagnamento alla Sicurezza" di AGID, consiste nella assistenza nella autovalutazione dei rischi, eseguita mediante un apposito "tool", che consente chiaramente di individuare le priorità di intervento per la riduzione del rischio: ciò non toglie che una PA possa chiedere una assistenza immediata nella riduzione di un rischio giudicato prioritario, salvo poi completare il risk assessment.

Non costituisce tutto ciò un esempio da imitare?

Anthony.wright@anssaif.it

https://www.key4biz.it/agid-continua-a-spingere-in-alto-la-resilienza-della-pa-agli-attacchi-cyber/259566/

Exodus, come è andata a finire la spystory (due

arresti)

Sono scattati due arresti per la vicenda del malware **Exodus**, lo spyware made in Italy impiegato dalle procure e attraverso il quale sarebbero state spiate diverse centinaia di utenti senza la preventiva autorizzazione della magistratura.

Un amministratore e un tecnico della ditta informatica calabrese che ha sviluppato il software sono stati arrestati a seguito delle indagini condotte dal Ros, dal Nucleo speciale tutela frodi tecnologiche della Guardia di Finanza e della Polizia Postale. Le indagini sono state coordinate dal pool cybercrime della Procura della Repubblica di Napoli, coordinato dal procuratore Giovanni Melillo.

La storia di Exodus

Lo spyware – sviluppato dalla società calabrese **eSurv** – 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.

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.

Gli arresti

All'amministratore delegato della società calabrese e al tecnico, ora ai domiciliari, vengono contestati i reati di intercettazione illegale e accesso abusivo a sistema informatico. Secondo una prima stima degli inquirenti, su 898 inoculazioni del virus spia, 234 non erano autorizzate dall'autorità giudiziaria.

I rischi privacy per gli utenti

Anche il Presidente del Garante per la protezione dei dati personali, **Antonello Soro,** ha espresso tutte le sue perplessità riguardo la vicenda legata al caso Exodus, in modo particolare sui tanti pericoli da evitare sul tema delle intercettazioni e tecnologie, dichiarando la necessità di introdurre un intervento normativo per aiutare gli utenti a proteggere la propria privacy.

I recenti sviluppi del "caso Exodus" ripropongono, sotto aspetti diversi, il tema delle intercettazioni. La notizia dell'accesso agli atti di centinaia di inchieste e dell'intercettazione di altrettanti cittadini del tutto estranei ad indagini dimostra il grado di pericolosità di strumenti investigativi fondati, come nel caso dei trojan, su tecnologie particolarmente invasive", ha dichiarato recentemente in un suo intervento **Soro.**

"Se rese disponibili sul mercato in assenza – dolosa o colposa – dei filtri necessari a limitarne l'acquisizione da parte dei terzi, queste app rischiano, infatti, di trasformarsi in pericolosissimi strumenti di spionaggio massivo. È dunque ineludibile – come abbiamo indicato, anche di recente, al legislatore – un intervento normativo che rafforzi le garanzie previste sul punto dalla (attualmente sospesa) riforma "Orlando", contrastando soprattutto i rischi connessi al coinvolgimento di soggetti diversi nella "catena" delle

indagini. Su un terreno che incrocia il potere investigativo e quello, non meno forte, della tecnologia, aggiunge il Garante Privacy, *le garanzie sono irrinunciabili: mai come in questo caso, infatti, costituiscono forma e sostanza della democrazia".*

https://www.key4biz.it/exodus-come-e-andata-a-finire-la-spystory-due-arresti/259536/

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/

New York Department of Financial Services Launches Cybersecurity Unit

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/dPe1QSkYjkk/new-york-department-financial-services-launches-cybersecurity-unit

---

Assange Charged With 17 New Counts Under Espionage Act

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/bQ_U8n6GPyc/assange-charged-17-new-counts-under-espionage-act

---

Facebook Figures Five Percent of Accounts Are Fake

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/mu_pX2r3vFA/facebook-figures-five-percent-accounts-are-fake

---

US Officials Say Foreign Election Hacking Is Inevitable

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/vau1_vZIShc/us-officials-say-foreign-election-hacking-inevitable

Instagram Says Not Source of Contact Info for Influential Users

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/NjHgYZIQgZs/instagram-says-not-source-contact-info-influential-users

Authorities Take Down Cryptocurrency Mixing Service Bestmixer.io

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/hkji4yD2jrI/authorities-take-down-cryptocurrency-mixing-service-bestmixerio