World’s Largest Beer Brewer Sets Up Cybersecurity Team

AB InBev controls over 400 beer brands including Budweiser, Corona and Stella Artois, but faces so many attacks it needs a dedicated cybersecurity unit to protect the business.

June 13, 2019 2 min read

This story originally appeared on PCMag

If a reminder were needed that nobody is immune to the threat of cyberattacks, the world’s largest brewer of beers has felt the need to establish its own cybersecurity division.

Anheuser-Busch InBev (AB InBev) controls over 400 different brands of beer including Budweiser, Corona, Stella Artois, Beck’s. Hoegaarden and Leffe. It’s a huge player in the market as a multinational drinks company, and as Reuters reports, it felt the need to protect itself from attack. The company’s solution is to setup a dedicated cybersecurity unit in Israel, which is widely viewed as a leader in online security and threat detection.

Luis Veronesi, AB InBev’s vice president of global security and compliance, explained that, “With increasing digitalization, we have to be prepared to defend against anything coming.” The cybersecurity office is located in Tel Aviv and will be fully-focused on discovering potential attacks against the company before they happen as well as analyzing any threats.

The move to protect itself online isn’t without cause. Veronesi admits the company is already facing regular attacks that are either attempting to disrupt operations or force the

company to pay up, suggesting ransomware remains a big threat for businesses.

Locating the team in Israel makes sense when you consider AB Inbev already operates there after acquiring Israel-based startup Weissberger last year. Weissbeerger collects data in real-time regarding beer consumption at the point of sale using the internet. Now its operations will be protected by this new cybersecurity unit.

As I'm sure many of my fellow beer drinkers around the world will agree, AB InBev's move to protect itself and keep the beer flowing should be welcomed and copied across the industry.

https://www.entrepreneur.com/article/335241

Cybercrime, Raoul Chiesa: vi spiego perché è in atto l'Hackmageddon

Un team di hacker potrebbe mettere in ginocchio un Paese, bloccando autostrade, aerei, banche, treni. Insomma uno scenario apocalittico, uno scontro finale: il cosiddetto **Armageddon.**

Non è fantascienza, ma una possibilità, secondo **Raoul Chiesa**, uno dei primi hacker etici italiani, celebre con lo pseudonimo di "Nobody", che ha parlato di '**Hackmageddon**' durante l'evento **Connecting The Future,** del **Consortium Garr** organizzato dal **Politecnico di Torino.**

Durante il suo intervento, ripreso in un'articolo de **La**

Stampa, Chiesa sostiene che “*La guerra mondiale è in atto e l’Italia è impreparata. Il nostro Paese subisce attacchi silenziosi e invisibili: ci vengono rubati dati e proprietà intellettuali* – spiega l’hacker etico -. *Purtroppo non contrattacchiamo come fanno le altre nazioni, e, invece, dovremmo andare a capire chi ci attacca e cosa ci ruba. Altrimenti rimaniamo in ginocchio, ammanettati e bendati.*“

Poi aggiunge: ” *Non basta scoprire l’indirizzo Ip: servono tecniche di tracciamento per capire chi c’è dietro. Serve una nuova generazione di di diplomatici cibernetici che spiegano ai ministri come muoversi. Non c’è ancora una leglislazione di guerra applicata agli attacchi cyber*“.

Le infrastrutture critiche il vero obiettivo

Secondo l’esperto “*Le infrastrutture critiche sono i principali obiettivi del crimine informatico, in modo particolare porti, aeroporti e stazioni. Nessuno credeva sarebbe stato possibile sabotare una centrale energetica, fino a quando è successo in* ***Ucraina****. Con l’Internet Of Things saremo sempre più esposti. Le vittime però non sono solo le infrastrutture critiche. Abbiamo dimostrato* – continua Chiesa – *che è possibile da remoto variare i dosaggi di una pompa di insulina e uccidere il paziente. Si può entrare nel sistema di un ospedale. cambiare una cartella medica o rubare informazioni e venderle alle assicurazioni”.*

Secondo l’hacker bisogna passare da un approccio teorico a uno pratico. “*Perché il web è come la sabbia: non è stato progettato per la sicurezza, ma per essere sempre disponibile. E’ un errore pensare che la sicurezza risieda in un software,*

che è un insieme di approcci e processi. I cittadini non capiscono che, se una cosa è gratis, è il perché il prodotto è l'utente. Scrivere sui social ciò che si fa alimenta il sistema che usa i nostri dati".

https://www.key4biz.it/cybercrime-raoul-chiesa-vi-spiego-perche-e-in-atto-lhackmageddon/261511/

Riconoscimento facciale, attacco hacker alla frontiera Usa. Rubate 100mila foto

Come non detto. Il dibattito sull'utilizzo della tecnologia per il riconoscimento facciale da parte delle forze dell'ordine americane è più acceso che mai.

Qualche ora fa il **Washington Post** ha diffuso la notizia di un attacco hacker ha preso di mira un contractor della **Us Customs and Border Protection (Cbp)**, la principale agenzia Usa per la sicurezza delle frontiere, in servizio di controllo doganale e di transito presso i varchi di confine nazionale. Secondo le stime sarebbero coinvolte 100.000 persone da questo attacco informatico.

I rischi legati alla sicurezza del riconoscimento facciale

La società hackerata (un'azienda terzista) aveva archiviato i dati raccolti dalla Cbp, ovvero le informazioni personali dei viaggiatori, comprese le foto, i passaporti, le impronte digitali.

L’agenzia americana è venuta a conoscenza del 31 maggio che il subappaltatore aveva trasferito le immagini sulla sua rete. Il CBP non ha dichiarato quando la società ha trasferito le fotografie o quando si è verificato l’attacco informatico.

Il CBP aveva raccolto le immagini dei viaggiatori negli aeroporti e ai valichi di frontiera. Ha anche iniziato a utilizzare il riconoscimento facciale per identificare i viaggiatori, compresi quelli che cercano di entrare illegalmente nel paese.

L’attacco informatico si è verificato proprio mentre “*La Cbp sta espandendo il suo enorme apparato per il riconoscimento facciale e per la raccolta di informazioni sensibili dei viaggiatori, come le informazioni sulle targhe o gli identificatori sui social media*“, ha denunciato **Neema Singh Guliani,** dell’American Civil Liberties Union (Aclu). “*Il modo migliore per evitare questo tipo di violazioni* – ha aggiunto – *è non raccogliere ed archiviare questi dati*“.

Facial ID: un problema di privacy

Negli Usa, l’uso del riconoscimento facciale da parte delle agenzie governative, sta sollevando nuove domande sulla privacy e sulla sicurezza dei dati. Ieri abbiamo dato la notizia del lancio di un nuovo sito chiamato AirlinePrivacy.com ad opera di un gruppo di attivisti della privacy, che mostra agli utenti quali compagnie aeree utilizzano il riconoscimento facciale per verificare l’identità dei passeggeri prima dell’imbarco in aeroporto.

Il progetto, nato a difesa e tutela dei diritti dei viaggiatori, aiuta inoltre i clienti a prenotare voli direttamente con compagnie aeree che non utilizzano questo tipo di tecnologie invasive.

Lo scorso maggio la città di **San Francisco** ha votato per metterne al bando l'utilizzo da parte della polizia. E' la prima città Usa ed altre municipalità americane stanno pensando di seguirne le orme.

Per approfondire

https://www.key4biz.it/riconoscimento-facciale-attacco-hacker-alla-frontiera-usa-rubate-100mila-foto/261291/

In Gazzetta Ufficiale il Cybersecurity Act europeo, entrerà in vigore il 27 giugno prossimo

Lo scorso venerdì, 7 giugno, è stato pubblicato nella **Gazzetta ufficiale dell'Unione europea** l'atteso ***Cybersecurity Act,*** il Regolamento europeo sulla cyber sicurezza, tra certificazioni, standard e tecnologie, che **entrerà in vigore formalmente il prossimo 27 giugno 2019**.

Il Cybersecurity Act, "*allo scopo di garantire il buon funzionamento del mercato interno perseguendo nel contempo un elevato livello di cibersicurezza, ciberresilienza e fiducia all'interno dell'Unione*", stabilisce nell'Articolo 1 alcuni punti chiave per definire al meglio tra i Paesi dell'Unione "*gli obiettivi, i compiti e gli aspetti organizzativi relativi all'**ENISA***", ad esempio, l'Agenzia dell'Unione europea per la *cybersicurity*; ma anche per "*definire un quadro regolatorio per l'introduzione di sistemi europei di certificazione della cyber sicurezza*", al fine di garantire un livello adeguato di

sicurezza dei prodotti e i servizi relativi al settore delle tecnologie per l'informazione e la comunicazione (Tic) nell'Ue; oltre che al fine di "*evitare la frammentazione del mercato interno*" per quanto riguarda i sistemi di certificazione della cibersicurezza nell'Unione.

Il regolamento, che dà anche una definizione ufficiale per cibersicurezza ("*l'insieme delle attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche*"), prevede inoltre che alcuni articoli, come il 58, il 60 e il 61, il 63, il 64 e il 65, entreranno in vigore tra un anno, delegando alle autorità nazionali di certificazione della cybersecurity.
L'accordo definitivo sul testo era arrivato a dicembre 2018, mentre l'intesa politica tra le Istituzioni europee sul Regolamento è stata trovata a marzo 2019, con il potenziamento del dispositivo della cyber sicurezza europea e il rafforzamento dell'ENISA stessa.

In termini di coordinamento con gli Stati membri e di maggiore dotazione di risorse, il "*Cybersecurity Act*" prevede per l'Agenzia europea per la sicurezza delle reti e dell'informazione: un mandato permanente per l'Agenzia in sostituzione dell'attuale mandato limitato (che sarebbe scaduto nel 2020), oltre a una maggiore dotazione di risorse per consentire all'agenzia di raggiungere i suoi obiettivi; una base più solida per l'ENISA nel nuovo quadro di certificazione della cibersicurezza per coadiuvare gli Stati membri a rispondere efficacemente agli attacchi informatici, prevedendo un ruolo più forte nella cooperazione e nel coordinamento a livello dell'Unione.
L'ENISA, infine, costituirà un centro indipendente di competenze "*che contribuirà a promuovere un elevato livello di consapevolezza presso il pubblico e le imprese, coadiuvando al contempo le istituzioni dell'UE e gli Stati membri nell'elaborazione e nell'attuazione delle politiche*".

Sul Regolamento abbiamo sentito **Paolo Dal Cin**, Managing Director di Accenture Security e Security Lead per l'Europa e l'America Latina (EALA), che ha affermato: "*Il livello di standardizzazione in Europa in tema di cybersecurity è ancora molto basso. In questo contesto il Cybersecurity Act rappresenta sicuramente un passo importante per poter garantire, da un lato un modello operativo che abiliti una collaborazione snella e efficace tra tutti i soggetti all'interno della comunità europea, dall'altro un sistema di certificazione di riferimento che assicuri una protezione adeguata di tutti i prodotti e servizi digitali. Sono tutti elementi che riteniamo indispensabili per mantenere alto il livello di fiducia digitale dei consumatori e di tutto l'ecosistema*".
Sulla cybersecurity come strumento di protezione delle infrastrutture critiche nazionali ed europee e come opportunità per le imprese ed il mercato unico, **Dal Cin intervistato a marzo da Key4biz aveva dichiarato**: "*la cybersecurity non è un costo, ma opportunità di business per le aziende per abilitare nuove opportunità legate all'Innovazione*".

"*Con il Cyber Security Act inizia a prefigurarsi quella che sarà la risposta dell'Europa ad un massiccio aumento delle minacce informatiche esplose negli anni scorsi e cresciute in modo preoccupante.*
Si tratta di un testo fondamentale che pone l'ENISA come guida della cyber security europea e mette ogni Stato nella condizione di impegnarsi attivamente nel contrasto degli atti dolosi.
È un'Europa che vuole reagire e vuole avere una parte realmente attiva nella protezione dei dati e delle reti. Un segnale di cui avevamo veramente bisogno e che arriva nel momento di maggior bisogno per la sicurezza degli utenti e

delle istituzioni", ha commentato per Key4biz **Edoardo Limone**, Specialista ICT e Cyber Security Expert.

Il Cybersecurity Act, infine, consentirà la nascita di un "***Quadro europeo di certificazione***" all'interno del **Mercato unico digitale europeo** (Art. 46): al fine di migliorare le condizioni di funzionamento del mercato interno, "*aumentando il livello di cibersicurezza all'interno dell'Unione e rendendo possibile, a livello di Unione, un approccio armonizzato dei sistemi europei di certificazione della cibersicurezza allo scopo di creare un mercato unico digitale per i prodotti TIC, i servizi TIC e i processi TIC*".
Il quadro europeo di certificazione della cibersicurezza, infine, prevede un meccanismo volto a "*istituire sistemi europei di certificazione della cibersicurezza*" e ad "*attestare che i prodotti, servizi TIC e processi TIC valutati nel loro ambito sono conformi a determinati requisiti di sicurezza*", al fine di "*proteggere la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati, trasmessi o trattati o le funzioni o i servizi offerti da tali prodotti*".

https://www.key4biz.it/in-gazzetta-ufficiale-il-cybersecurity-act-europeo-entrera-in-vigore-il-27-giugno-prossimo/261090/

Cybercrime, in Italia la sanità resta il settore più colpito. In calo l'hacktivism

Nel 2018 gli attacchi informatici gravi sono aumentati del 38% su base annua raggiungendo la cifra di 1.552, pari a 129 attacchi al mese contro i 94 del 2017. La stragrande

maggioranza (1.232 attacchi) è rappresentata dal cybercrime, che “si evolve”. In calo l’hacktivism (hacker attivisti come Anonymous), passato dai 236 attacchi gravi del 2014 a 61 nel 2018.

I dati, elaborati dal **Clusit**, hanno evidenziato il 16% prende di mira gli enti governativi, mentre il 20%, uno su cinque, ha target multipli.

Lo studio evidenzia come i cybercriminali – sempre più attivi e organizzati che colpiscono target multipli cercando di massimizzare i profitti – prendono di mira soprattutto enti governativi e il settore sanitario, molto appetibile per via dei dati sensibili che custodisce. 1 attacco informatico su 10 infatti è indirizzato al settore, in cui gli attacchi sono raddoppiati tra il 2017 e il 2018.

“*La cybersicurezza non è una sicurezza per addetti ai lavori, oggi e’ una sicurezza generale, perché nel mondo digitale, in cui siamo completamente immersi, ci sono tutti gli aspetti della nostra vita. Quando parliamo dei dati come merce pregiata, oramai soggetta ad ogni tipo di trafugamento, sollecitazione e ad appetiti vari (leciti, illeciti, borderline), parliamo di dati nostri di vita, non di dati che hanno solo valore statistico*“. Lo ha dichiarato il Direttore del Servizio Polizia Postale e delle Comunicazioni **Nunzia Ciardi** nel corso del suo intervenuta ieri all’evento.

“*Dal 2017 al 2018* – ha ricordato il direttore – *abbiamo avuto un aumento di denunce del 340% di attacchi finanziari a grandi e piccole e medie aziende e un importo di frodi denunciate di +172%. Parliamo quindi di fenomeni che hanno un’incidenza forte sulla nostra economia. Se continuiamo a parlare di sicurezza informatica come di un tema per addetti ai lavori non si fa un favore alla collettivita’, ne’ restituiamo*

un’immagine vera. Questo è un attacco sistematico alle infrastrutture di un Paese“.

La Polizia Postale ha siglato recentemente due intese strategiche: **Zecca di Stato** e **Consob**. Gli accordi rientrano nell’ambito delle direttive impartite dal Ministro dell’Interno per il potenziamento dell’attività di prevenzione alla criminalità informatica con gli operatori che forniscono prestazioni essenziali ed infrastrutture critiche di interesse nazionale.

https://www.key4biz.it/cybercrime-in-italia-la-sanita-resta-il-settore-piu-colpito-in-calo-lhacktivism/260762/

Cybercrime, in Italia la PA è presa di mira da Ransomware, Banking Trojan e Spear Phishing

Gli attacchi informatici che colpiscono di più la Pubblica Amministrazione in Italia? **Ransomware**, **Banking Trojan** e campagne malevole mirate principalmente al furto di credenziali istituzionali chiamate **Sprear Phishing.**

Lo hanno rivelato gli esperti di cybersecurity del *Computer Emergency Response Team della Pubblica Amministrazione* (**CERT-PA**) – l’organo che ha il compito di supportare le amministrazioni nella prevenzione e nella risposta agli incidenti di sicurezza informatica – diffondendo i dati relativi alle minacce cibernetiche monitorate a maggio 2019.

Grafico rappresentativo degli eventi registrati e gestiti dal CERT-PA

I dati del CERT-PA evidenziano come la PA italiana sia stata attaccata con **Trojan**, come Ursnif e Gootkit, insieme al **ransomwame GandCrab** e al malware **Formbook**. In terza posizione si collocano, invece, i numerosi attacchi informatici di tipo Spear Phishing, mirati principalmente al furto di credenziali istituzionali. Non mancano nemmeno, comunque, **AdWare**, **Trojan** di altro tipo, **RAT**, **CryptoMiner**, **Bakdoor**, **Android** e **Infostealer**.

- Fonte: CERT-PA

Da queste analisi del CERT-PA sulle minacce in Italia, effettuate anche grazie al monitoraggio dei malware del ricercatore di cyber security **JAMESWT_MHT,** sono emersi elementi interessanti. Ad esempio le campagne di malspam con malware Ursnif si sono rilevate in molti casi "*fallate*": il link nel corpo delle mail era errato o il file allegato, solitamente uno zip, conteneva i file malevoli senza il payload utile a compromettere il sistema.

La cosa più interessante invece riguarda la cadenza, quasi una routine, delle campagne monitorate. Il CERT ha rilevato un'alternanza piuttosto regolare nella diffusione di specifici malware cadenzata nei giorni della settimana. Ad esempio, nello specifico caso di Ursnif, in certi giorni il malware può essere veicolato tramite link presente nel corpo delle mail, in altri diffuso tramite allegato DOC e giorni in cui viene utilizzato un allegato in formato XLS o VBS.

Attacchi per illeciti economici

Gli esperti hanno evidenziato come questo tipo di campagne cyber siano orchestrate da uno o più gruppi criminali il cui fine è quello di produrre, direttamente o meno, illeciti profitti economici a danno di utenti italiani.

Per massimizzare gli attacchi i cyber criminali abbiano escogitato una metodologia che consente loro di ottimizzare al meglio le operazioni, veicolando malware principalmente nei giorni feriali con una logica organizzativa che prevede una ricorsività nel metodo di diffusione;

Inoltre, gli errori emersi nelle campagne di malspam, nella catena di infezione e nell'utilizzo delle medesime credenziali di accesso ai server di C&C, lasciano presupporre, con buona probabilità, che i criminali non siano gli stessi autori del malware ma utilizzino infrastrutture esistenti, spesso disponibili a noleggio presso i black market, puntando principalmente a compromissioni di tipo massivo.

https://www.key4biz.it/cybercrime-in-italia-la-pa-e-presa-di-mira-da-ransomware-banking-trojan-e-spear-phishing/260475/

Lotta al cybercrime, al via l'alleanza tra Consob e Polizia di Stato

Continua senza sosta l'impegno della **Polizia di Stato** nella lotta e tutela dei cittadini nel settore della cybersecurity. Oggi è stato firmato un nuovo accordo con la Commissione nazionale per le società e la Borsa **(Consob)** sulla prevenzione

e il contrasto dei crimini informatici che hanno per oggetto i sistemi e i servizi informativi di particolare rilievo per il Paese.

La convenzione – che arriva quasi una settimana dopo la firma tra la Polizia postale e **l'Istituto Poligrafico e Zecca dello Stato** – è stata firmata dal Presidente della Consob, **Paolo Savona**, e dal Capo della Polizia **Franco Gabrielli.**

Questa operazione rientra nell'ambito delle direttive impartite dal Ministro dell'Interno per il potenziamento delle attività di prevenzione della criminalità informatica attraverso la stipula di accordi con gli operatori che forniscono prestazioni essenziali.

La Polizia Postale e delle Comunicazioni è, infatti, quotidianamente impegnata a garantire l'integrità e la funzionalità della rete informatica delle strutture di livello strategico per il Paese attraverso il **Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche.**

La Consob, nella sua attività di regolamentazione e di vigilanza sui mercati finanziari, ricopre un ruolo determinante e rappresenta un'infrastruttura di interesse nazionale. Pertanto, la protezione dei suoi sistemi informatici è da considerarsi necessaria per assicurare il pieno svolgimento delle sue funzioni.

L'accordo, basato sulla condivisione informativa e sulla cooperazione operativa, ha durata triennale e rappresenta una tappa significativa nel contrasto al *cybercrime.*

Alla firma della convenzione erano anche presenti, per il Dipartimento della Pubblica Sicurezza, il Direttore Centrale per la Polizia Stradale, Ferroviaria, delle Comunicazioni e

per i Reparti Speciali della Polizia di Stato, **Armando Forgione**, e il Direttore del Servizio Polizia Postale e delle Comunicazioni, **Nunzia Ciardi**; per la Consob il Commissario **Paolo Ciocca**, il Segretario Generale, **Carlo Deodato**, il Responsabile Divisione Infrastrutture Informative, **Paolo Libri**, e il Responsabile Ufficio Sicurezza Informatica, **Claudio Gentili.**

https://www.key4biz.it/lotta-al-cybercrime-al-via-lalleanza-tra-consob-e-polizia-di-stato/260359/

Polizia Postale e Zecca di Stato insieme per il contrasto dei crimini informatici

E' stato siglato a Roma l'accordo tra **Polizia di Stato** e l'**Istituto Poligrafico e Zecca dello Stato S.p.A**., per la prevenzione e il contrasto dei crimini informatici che hanno per oggetto i sistemi e i servizi informativi di particolare rilievo per il Paese, quali infrastrutture critiche di interesse nazionale.

La convenzione, firmata dal Capo della Polizia-Direttore Generale della Pubblica Sicurezza, **Franco Gabrielli**, e dall'Amministratore Delegato dell'Istituto Poligrafico e Zecca dello Stato S.p.A., **Paolo Aielli**, rientra nell'ambito delle direttive impartite dal Ministro dell'Interno per il potenziamento dell'attività di prevenzione alla criminalità informatica attraverso la stipula di accordi con gli operatori che forniscono prestazioni essenziali.

Paolo Aielli, Amministratore Delegato dell’Istituto Poligrafico e Zecca dello Stato S.p.A. e
Franco Gabrielli, Capo della Polizia-Direttore Generale della Pubblica Sicurezza
La Polizia Postale e delle Comunicazioni è infatti quotidianamente impegnata a garantire l’integrità e la funzionalità della rete informatica delle strutture di livello strategico per il Paese attraverso il Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche.

L’Istituto Poligrafico e Zecca dello Stato S.p.A realizza e sviluppa sistemi per la sicurezza e per la garanzia della Fede Pubblica, attraverso tecnologie all’avanguardia che garantiscono l’identità fisica e digitale dei cittadini, avvalendosi di sofisticati sistemi di anticontraffazione e tracciabilità. Queste attività che fanno del Poligrafico una realtà tecnologica evoluta e uno dei principali partner istituzionali operativi a supporto della Pubblica Amministrazione, richiedono dei livelli di sicurezza sempre più elevati, a garanzia dell’integrità dei sistemi informatici, tecnologici e delle reti telematiche.

Il **CNAIPIC**, che da anni si occupa della tutela delle reti informatiche di realtà sia pubbliche che private, di rilievo nazionale e di importanza strategica per il Paese, risulta quindi essere uno strumento necessario di collaborazione e di condivisione delle informazioni su tutto il territorio nazionale.

Alla firma della convenzione erano presenti per il Dipartimento della Pubblica Sicurezza, il Direttore Centrale per la Polizia Stradale, Ferroviaria, delle Comunicazioni e

per i Reparti Speciali della Polizia di Stato, **Armano Forgione** e il Direttore del Servizio Polizia Postale e delle Comunicazioni, **Nunzia Ciardi**. Mentre per l'Istituto Poligrafico e Zecca dello Stato S.p.A il Responsabile Direzione Sistemi di Prevenzione e Tutela aziendale, **Marco Ferraro** e il Responsabile Affari Istituzionali e Comunicazione, **Sabrina Romani.**

https://www.key4biz.it/polizia-postale-e-zecca-di-stato-insieme-per-il-contrasto-dei-crimini-informatici/259971/

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/