Lavorare come hacker etico, che significa: la certificazione CEH

Anita Biscaro

UNIVERSITÀ
DEGLI STUDI
FIRENZE

Research Analysis

Marzo 2018

Center for Cyber Security and International Relations Studies (CCSIRS)

Centro Interdipartimentale di Studi Strategici, Internazionali e Imprenditoriali (CCSSII)

Università degli Studi di Firenze

Via delle Pandette 2, 50127, Firenze

https://www.cssii.unifi.it/ls-6-cyber-security.html

Center for Cyber Security and International Relations Studies

Lavorare come hacker etico, che significa: la certificazione CEH

Anita Biscaro

UNIVERSITÀ DEGLI STUDI FIRENZE

Research Analysis

Marzo 2018

Riguardo all’autore

Anita Biscaro Si è laureata in Studi Internazionali presso l'Università degli Studi di Trento con una tesi sulla crisi di legittimazione delle istituzioni europee. Ha studiato presso il Barnard College della Columbia University a New York ed è attualmente iscritta al Master's degree in International Security Studies presso la Scuola Sant'Anna di Pisa. Si interessa principalmente di Cyber Policy a livello europeo, con focus sul rapporto tra settore pubblico e privato. É autrice degli articoli "Cyber and Human Vulnerabilities" e "Lavorare come Hacker Etico" pubblicati rispettivamente su SecurityPraxis.eu e AgendaDigitale.it.

Lavorare come hacker etico, che significa: la certificazione CEH[1]

La Certified Ethical Hacker (CEH), è una certificazione promossa International Council of Electronic Commerce Consultants, noto come EC-Council[2]. Va incontro alle esigenze di chi vuole lavorare come hacker etico o di chi vuole assumere questa figura. Affronta una questione ancora controversa. La categoria hacker, com'è noto, non è più popolata solo da malevoli *"black hat"* o *"unethical hackers"*, ma anche da individui che mettono le proprie conoscenze tecniche a servizio della comunità per aumentarne – e non diminuirne – la sicurezza collettiva. Questi ultimi vengono chiamati ***"white hat"*** o *"ethical hackers"*, gli hacker etici.

La loro attività consiste nel simulare gli attacchi di hacker maligni con lo scopo di trovare prima di essi le vulnerabilità nei sistemi, cercando di risolvere i problemi riscontrati. Il loro scopo è quindi quello di contrastare le attività criminali degli hacker non etici conducendo azioni guidate da una scelta morale individuale, o, sempre più frequentemente, perché richiesto dal loro contratto di lavoro. Il crescente numero e la crescente complessità degli attacchi informatici subiti da aziende e governi, infatti, sta aumentando le richieste di assunzione di hacker etici. Allo stesso modo, per gli informatici esperti, dotati di solide conoscenze e buona reputazione nel settore, la carriera dell'hacking etico sta diventando una scelta professionale sempre più comune.

[1] La seguente analisi è apparsa su https://www.agendadigitale.eu/ il giorno 29 marzo 2018 ed è reperibile al seguente link: https://www.agendadigitale.eu/sicurezza/lavorare-come-hacker-etico-che-significa-la-certificazione-ceh/.
[2] https://www.eccouncil.org/about/

CEH: Certified Ethical Hacker Certification

Gli hacker etici, quindi, sono una categoria sempre più richiesta da aziende e governi consapevoli della necessità di proteggere efficacemente le proprie infrastrutture da possibili attacchi informatici. Questi ultimi, infatti, potrebbero compromettere la produzione di beni e servizi chiave per tutta la comunità. Per questo motivo un crescente numero di datori di lavoro richiede ai potenziali impiegati di diventare Certified Ethical Hacker**,** tramite una certificazione che mira a garantire che l'hacker non solo padroneggia la tecnologia, ma comprende anche le responsabilità etiche dell'impiego. Partendo dal presupposto che molti datori di lavoro non hanno le competenze per valutare le capacità dei candidati, questa certificazione ha lo scopo assicurare che i potenziali impiegati siano tecnicamente e moralmente qualificati.

La Certified Ethical Hacker (CEH), è una certificazione promossa International Council of Electronic Commerce Consultants, noto come EC-Council**.** L'organizzazione è stata fondata in seguito agli attacchi al World Trade Center dalla volontà di Jay Bavisi e Haja Mohideen di formare adeguatamente professionisti nel campo della sicurezza informatica. Il loro obiettivo era quello di educare e di fornire gli strumenti adatti ad individui che sarebbero stati capaci di evitare – e, nel caso – affrontare, una guerra cyber. Le attività dell'EC-Council hanno da subito beneficiato del sostegno di esperti del settore provenienti da tutto il mondo ed in breve tempo l'organizzazione è stata in grado di fissare standard internazionali certificando diverse competenze tecniche nei campi dell'E-commerce e della sicurezza informatica. La CEH ricade in quest'ultima categoria. È attualmente disponibile in più di 60 paesi diversi, riconosciuta internazionalmente ed è stata recentemente avallata da diverse agenzie governative statunitensi, come US Government National Security Agency (NSA)

e la Committee on National Security Systems (CNSS). Negli Stati Uniti, la certificazione è posseduta da professionisti impegnati in settori chiave quali l'esercito e l'FBI. Il test si compone di 125 domande a risposta multipla da completare in 4 ore e comprende l'accettazione di 19 regole che compongono il Codice Etico dell'organizzazione quali "Proteggi la proprietà intellettuale", "Usa le proprietà del cliente o del datore di lavoro solo nei modi e tempi autorizzati", "Non fare parte di comunità hacker con lo scopo di diffondere e promuovere attività *black hat*".

Da una parte, la CEH è uno strumento essenziale per attestare le capacità degli individui ed è la dimostrazione di un tentativo di standardizzazione promosso sia dal settore pubblico che quello privato, dall'altra parte, però, i detrattori della certificazione criticano la sua vana aspirazione di certificare anche la virtuosità delle intenzioni dei candidati, una caratteristica che – secondo i critici – appartiene alla soggettività degli individui, e non può quindi rientrare in standard oggettivi. Inoltre, la CEH certifica il possesso da parte dei soggetti degli strumenti e delle conoscenze possedute anche dai *black hat hackers*: con il corso che precede la certificazione e con la certificazione stessa, quindi, si promuove l'apprendimento di tecniche potenzialmente criminali da parte di un ampio numero di persone.

Sul sito ufficiale dell'EC-Council, è presente una sezione riguardante le domande frequenti, in cui si possono trovare le confutazioni alle precedenti obiezioni. Innanzitutto, l'EC-Council specifica che il corso che precede la certificazione è accessibile solamente da persone che abbiano già almeno due anni di esperienza nel campo della sicurezza informatica, e sottolinea la difficoltà dell'esame, superabile solamente da chi ha solide conoscenze. La risposta, in questo caso, non appare sufficiente in quanto sia hacker con buone che con cattive intenzioni posso essere in possesso di precedente esperienza lavorativa e

soprattutto possono entrambi presentare lo stesso alto livello di conoscenza tecnica necessario per superare l'esame. Nonostante i tentativi di rispondere alle critiche, quindi, le controversie sono lontane dall'essere efficacemente chiarite, e queste sono principalmente imperniate sulla difficile distinzione tra hacker etici e hacker non etici.

Hacker etici e non etici: storiche somiglianze e nuove differenze

La difficoltà nella distinzione è dovuta al fatto che i due gruppi hacker sono accomunati da importanti somiglianze: sia white hat (ossia hacker etici) che *black hats* (gli hacker non etici) sono generalmente impersonati da individui con sofisticate conoscenze informatiche, e lo scopo di entrambi è cercare vulnerabilità nei sistemi, ossia imperfezioni che possono comprometterne il funzionamento. Per la ricerca delle vulnerabilità, inoltre, hacker etici e non etici ricorrono alle stesse tecniche e agli stessi strumenti.

La sostanziale differenza tra i due gruppi riguarda le diverse intenzioni dei soggetti rispetto alla vulnerabilità individuata: i primi – autonomamente o per contratto – mirano a sanare il difetto, per evitare che venga trovato da hacker non etici e sfruttato per diverse ragioni, da vantaggi economici a motivi personali. Il problema chiave è che, se le azioni possono essere facilmente valutate, le intenzioni – seppur centrali in questo contesto – possono essere identificate e giudicate solamente a posteriori.

La necessità distinzione tra hacker etici e non etici risale a ben prima dell'istituzione della CEH, anche se la comunità hacker è nata come un gruppo piuttosto omogeneo comprendente studenti dell'MIT accomunati dalla passione per la programmazione. Gli inizi della comunità hacker risalgono agli anni '60, e possono essere descritti a

partire dall'intrecciarsi di quattro filoni risalenti al momento in cui internet è diventato accessibile dal grande pubblico. Innanzitutto, il mondo cyber è diventato uno *spazio,* un luogo che – anche se non fisicamente accessibile – permetteva alle persone di entrare in contatto e di costruire un sistema condiviso di valori, un'etica comune. Contemporaneamente, nasceva la dottrina hacker del *"do-it-yourself"*: "fallo da solo", rappresentativa dell'attitudine alla libera manipolazione di dati e informazioni. Dalla somma di questi prime due tendenze, si è costituita la comunità virtuale hacker. Se inizialmente le interazioni erano di natura unicamente testuale, con il passare del tempo, lo spazio virtuale ha permesso l'instaurazione di relazioni sociali che hanno dato vita ad una vera e propria collettività fisica. Il quarto e ultimo filo conduttore corrisponde alla nascita della programmazione come professione e potenziale fonte di guadagno regolamentata e legale. In questo contesto sono nate anche sottocomunità e sottoculture, capaci di avvicinare individui con la volontà di superare emarginazione e di accorciare le distanze con il resto del mondo. Tra le varie comunità istituitesi spontaneamente sulla base di interessi condivisi, è nata la comunità hacker.

Se inizialmente la comunità hacker è apparsa come un gruppo uniforme, qualche decennio dopo, all'inizio degli anni '90, diversi studiosi hanno capito l'importanza di tracciare sotto categorie interne sulla base degli intenti degli hacker. Angerfelt, nel 1992, ha classificato 8 diverse forme di crimini informatici annoverando l'hacking tra questi. In seguito, Young ha suddiviso gli hacker in "utopici", ossia coloro che intendono aiutare la società identificando vulnerabilità e "cyberpunk", coloro che scelgono intenzionalmente di causare danni alle istituzioni e agli apparati burocratici. Infine, Denning ha adottato un punto di vista più pratico, dividendo gli hacker tra tradizionali (ossia, intrinsecamente benevoli) e maligni.

Nonostante i primi embrionali tentativi di stabilire differenziazioni interne al gruppo hacker, la comunità nel suo complesso ha conosciuto i propri "anni d'oro" verso la fine degli anni novanta, quando la già affermata idea del cyberspazio come un vero e proprio "luogo" caratterizzato da comunità nate spontaneamente, da un insieme di valori e da precise tecniche utilizzate per manipolare informazioni fa emergere la visione dell'attività di hacking prevalentemente come esplorazione intellettuale. Questa nobile causa diventa un elemento centrale durante gli anni d'oro dell'hacking, allo stesso tempo, però, in questo periodo si moltiplicano i casi di crimini informatici. Permane in questo periodo la difficoltà nel distinguere le azioni virtuose da quelle malevole, con la conseguente criminalizzazione di entrambi i gruppi hacker, senza tenere in considerazione gli intenti celati dietro le azioni.

Gli anni duemila rappresentano un cruciale momento di scissione della comunità hacker. Durante l'inizio del ventunesimo secolo, infatti, gli hacker sono protagonisti di quattro diverse tendenze che hanno portato ad una piuttosto radicale suddivisione interna della comunità. Le quattro tendenze sono:

- l'emergere di nuovi crimini informatici, e la conseguente crescita del gruppo di cyber criminali,
- l'affermarsi dell'attivismo hacker o *"hacktivism"*,
- l'istituzione di un nuovo legame tra attività hacker e economia capitalista, che ha dato vita ad una nuova classe lavorativa di hacker al servizio delle imprese,
- e infine l'idea che le attività hacker siano un'espressione di creatività confacente alla nuova moderna società che si stava delineando, che ha sancito la celebrazione dell'hacker come una sorta di "virtuoso del web".

In primo luogo, la nascita di giochi d'azzardo online è stata responsabile del collegamento tra crimine organizzato e gang criminali presenti del cyberspazio. L'unione ha dato vita a nuovi e pervasivi crimini online quali *botnets*, e ransomware, capaci di "infettare" computer di privati e di renderli inutilizzabili fino al pagamento di una somma di denaro. Di conseguenza, in questo periodo la polizia comincia ad impiegare maggiori risorse della ricerca e persecuzione dei cyber-criminali.

In secondo luogo, a differenza dei periodi precedenti, il nuovo millennio assiste alla nascita di hacker che compiono le proprie azioni sulla base di convinzioni etiche e/o politiche. Il fenomeno Anonymous è forse l'esempio più significativo di azioni compiute online e mirate a trasportare dimostrazioni di disobbedienza civile e manifestazioni di massa dalle piazze fisiche alle piazze virtuali. Allo stesso tempo, i gruppi composti da *hacktivists* quali Anonymus, hanno iniziato in questo periodo a cercare di accedere ad informazioni classificate per poi divulgarle al grande pubblico.

In terzo luogo, la comunità hacker, inizialmente indipendente ed autonoma, comincia, con l'affermarsi della tecnologia Open Source per lo sviluppo attività economiche, ad essere associata al mondo del profitto capitalistico.

Infine, il ventunesimo secolo è stato protagonista della celebrazione delle attività hacker come elemento positivo che rispecchiava l'affermarsi di una società nuova, moderna e aperta, in cui la manipolazione di informazioni era indice di una creatività sempre più promossa ed incoraggiata.

Gli hacker oggi: scomodi ma popolari dipendenti di governi e industrie

Attualmente, le attività degli hacker sono diventate accettate e diffusamente utilizzate sia da industrie sia da governi. Periodicamente, inoltre, diverse agenzie statali promuovono competizioni hacker al fine di trovare nuovi talenti da poter mettere al servizio della comunità. In questo modo si è consolidato il rapporto tra hacker e settore pubblico, il quale assolda individui specializzati in attività hacker sia per condurre azioni contro gli altri stati nella forma di cyber spionaggio e cyber sabotaggio, sia per promuovere una maggiore sicurezza collettiva tramite la protezione di infrastrutture critiche.

In realtà, l'assunzione di hacker etici crea problemi di tipo pratico e normativo. Da una parte, governi e industrie mirano ad assicurare solide misure di sicurezza per cercare di rendere sia il settore pubblico che quello privato immune, o meglio, resiliente, in caso di attacco cyber. Dall'altra parte, però, i tentativi di garantire tali misure di sicurezza rispettando leggi e principi democratici, si scontra con la natura intrinsecamente illegale delle attività degli hacker etici. Anche se autorizzati infatti, le azioni degli hacker etici violano diritti fondamentali quali il diritto alla privacy, la libertà di espressione, diritti commerciali e del consumatore. Inoltre, esiste un paradosso per il quale nella teoria il lavoro degli hacker etici dovrebbe puntare a rafforzare i principi chiave della sicurezza cibernetica ossia riservatezza, integrità e disponibilità delle informazioni, ma in realtà, usando gli stessi strumenti illegali degli hacker non etici, sia i primi che i secondi possono accedere, modificare e negare l'accesso alle informazioni, indebolendo tutti i suddetti principi.

Controversie irrisolte

Per questo motivo la Certified Ethical Hacker Certification appare necessaria: datori di lavoro pubblici e privati necessitano una

garanzia non solo rispetto alle capacità, ma anche rispetto buone intenzioni degli hacker etici assunti**.** Questa richiesta però, come già accennato, è solo parzialmente soddisfatta dalla CEH. La certificazione, infatti, appare solo come un primo tentativo di risolvere il ben più radicato problema della distinzione delle *intenzioni* che guidano le azioni degli hacker. Come dimostrato dagli eventi chiave che hanno caratterizzato la storia della comunità hacker, sin dalla sua nascita, questo gruppo si è contraddistinto per la volontà di preservare il proprio individualismo ed indipendenza nella scelta ed accettazione di valori e tecniche condivise. Allo stesso tempo però, con il passare dei decenni, la comunità si è dovuta confrontare con divisioni interne e con pressioni esterne, provenienti dal settore economico e politico, risultanti in una sempre maggiore interdipendenza tra il mondo virtuale e il mondo reale, portando gli hacker dall'essere una categoria confinata del cyber spazio ad una vera e propria classe lavorativa, con sempre più possibilità di impiego.

I problemi di fondo, però, restano. Innanzitutto, la CEH si basa sull'assunto che ci sia la possibilità di riconoscere principi etici universalmente condivisi tra tutti gli aspiranti hacker etici che desiderano ottenere la certificazione. Inoltre, forse ancora più significativamente, la garanzie delle buone intenzioni dei candidati viene assicurata tramite l'accettazione di un codice di condotta che rappresenta solamente una parte marginale della certificazione: se le competenze tecniche vengono attestate sulla base di 125 domande, la verifica delle "competenze morali" consiste solamente nella firma del codice etico[3] dell'EC-Council, composto da 19 punti. La CEH rappresenta un primo importante passo verso una collaborazione istituzionalizzata e standardizzata tra hacker e settori pubblico e privato, ma c'è ancora molta strada da fare, e non è priva di ostacoli.

[3] https://www.eccouncil.org/code-of-ethics/

Riferimenti bibliografici

Angerfelt. “Computer crimes. a study of different types of offences and offenders”. In *IFIP TC11 International Conference on Information Systems Security*, 1992.

Denning. “Concerning hackers who break into computer systems”. In *13th National Computer Security Conference*, 1990.

EC- Concil, “Certified Ethical Hacking Certification”. https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/

Leiwo, & S. Heikkuri, “An Analysis of Ethics as Foundation of Information Security in Distributed Systems”. *Proceedings of the Hawaii International Conference on System Sciences*, 6, 213-222, 1998.

L.F. Young. “Utopians, cyberpunks, players and other computer criminals”. In IFIP TC9/WG9.6 *Working Conference on Security and Control of Information Technology in Society*, 1993.

Jordan, “A genealogy of hacking Convergence: The International Journal of Research”. In *New Media Technologies*, Vol. 23(5) 528–544, 2017.

Center for Cyber Security and International Relations Studies (CCSIRS)

Centro Interdipartimentale di Studi Strategici, Internazionali e Imprenditoriali (CCSSII)

Università degli Studi di Firenze

Via delle Pandette 2, 50127, Firenze

https://www.cssii.unifi.it/ls-6-cyber-security.html