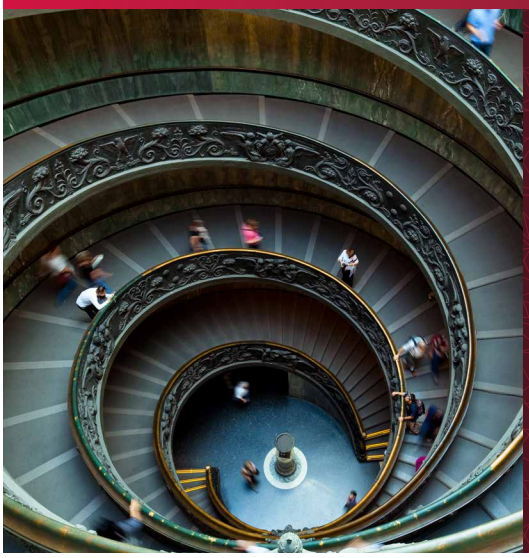

Sintesi del report

Perdite nette: stimare il costo complessivo del crimine informatico

L'impatto economico del crimine informatico II

Sintesi

Il crimine informatico è un settore in crescita. I ritorni sono fantastici e i rischi contenuti. Riteniamo che il costo annuale del crimine informatico per l'economia globale possa essere superiore ai 445 miliardi di dollari, includendo in questa cifra sia i guadagni per i criminali che i costi sostenuti dalle aziende per la protezione e le attività di ripristino. Una stima conservativa corrisponderebbe a una perdita di 375 miliardi di dollari, mentre quella massima potrebbe ammontare a 575 miliardi di dollari. Si tratta di cifre superiori al reddito nazionale della maggior parte delle nazioni ed equivale allo 0,5%-0,8% del reddito globale.

Dare un valore al costo legato al crimine e allo spionaggio informatico è l'inizio, ma è necessario porsi importanti domande sul danno per le vittime derivante dall'effetto cumulativo causato dalle perdite nel cyber spazio. Il crimine informatico include l'effetto di centinaia di milioni di persone che si vedono rubare le proprie informazioni. Una stima indica un totale di oltre 800 milioni di record individuali nel 2013, con un costo che potrebbe ammontare a 160 miliardi all'anno. La costante segnalazione di aziende violate contribuisce a una crescente sensazione di un crimine informatico fuori controllo.

Il costo più importante legato al crimine informatico, tuttavia, deriva dal danno causato alle prestazioni aziendali e alle economie nazionali. La nostra stima si basa su dati che tengono conto della perdita di proprietà intellettuale, del furto di risorse finanziarie e di informazioni di business riservate, costi legati alle opportunità, costi aggiuntivi per la protezione delle reti e il costo legato alle attività di ripristino a seguito di un attacco informatico, tra cui il danno alla reputazione di un'azienda violata. Le nostre fonti includono dati pubblici, interviste e stime effettuate da agenzie governative e aziende di tutto il mondo.

Abbiamo trovato centinaia di segnalazioni di aziende violate. Gli Stati Uniti, per esempio, hanno informato 3.000 aziende nel 2013 della violazione subita. Due banche nel Golfo Persico hanno perso 45 milioni di dollari. Un'azienda britannica ha segnalato di aver perso 1,3 miliardi di dollari. Le banche brasiliane affermano che i clienti perdono milioni ogni anno. Il CERT dell'India ha segnalato che 308.371 siti web sono stati violati tra il 2011 e il giugno 2013. Aggiungendo le perdite derivanti da incidenti noti, il totale raggiungerebbe miliardi di dollari e, purtroppo, esistono troppe storie da raccontare. Dato il numero di incidenti, sorprende che molte nazioni non si sforzino affatto di produrre stime ufficiali per le perdite legate al crimine informatico. E ciò è valido anche per le nazioni più grandi e sviluppate, ed è particolarmente vero per le nazioni con un reddito medio o basso. Questa mancanza naturalmente interessa tutti i tentativi di stimare le perdite con precisione.

Le nazioni del G20 soffrono della maggior parte delle perdite. Le perdite causate dal crimine informatico per le quattro principali economie al mondo (Stati Uniti, Cina, Giappone e Germania) hanno raggiunto i 200 miliardi. Le nazioni a basso reddito subiscono perdite inferiori, ma la situazione cambierà nel momento in cui tali nazioni aumenteranno il loro utilizzo di Internet e i criminali informatici inizieranno a sfruttare le piattaforme mobili. Per le nazioni sviluppate, il crimine informatico presenta serie implicazioni per l'occupazione. L'effetto è quello di allontanare l'impiego da impieghi che creano il valore maggiore. Il nostro primo report ha mostrato che le perdite derivanti dal crimine informatico potrebbero tradursi in oltre 200.000 impieghi persi negli Stati Uniti. Utilizzando i dati dell'Unione Europea, stimiamo che l'Europa potrebbe perdere quasi 150.000 impieghi a causa del crimine informatico. Se non è facile tradurre le perdite causate dal crimine informatico direttamente in perdita di impieghi, l'effetto sull'occupazione non può essere ignorato.

Le nazioni G20 soffrono della maggior parte delle perdite e le perdite causate dal crimine informatico per le quattro principali economie al mondo (Stati Uniti, Cina, Giappone e Germania) hanno raggiunto i 200 miliardi. Le nazioni a basso reddito subiscono perdite inferiori, ma la situazione cambierà nel momento in cui tali nazioni aumenteranno il loro utilizzo di Internet e i criminali informatici inizieranno a sfruttare le piattaforme mobili.

Il furto di proprietà intellettuale e la cannibalizzazione dell'innovazione

Le perdite in termini di proprietà intellettuale sono le più difficili da stimare per il costo del crimine informatico, ma è anche la variabile più importante per stabilire la perdita. Il furto di proprietà intellettuale cambia la bilancia commerciale e l'occupazione nazionale. Le nazioni dove i settori che creano e utilizzano proprietà intellettuale sono importanti per la creazione di ricchezza perdono di più in termini di attività commerciali, impieghi e guadagni a causa del crimine informatico. L'effetto dello spionaggio informatico sulla sicurezza nazionale è significativo e il valore monetario della tecnologia militare non riflette il costo complessivo per le nazioni vittime. Il crimine informatico danneggia l'innovazione. Un modo di considerare il costo legato al crimine informatico è chiedersi come gli investitori agirebbero se i ritorni sull'innovazione raddoppiassero. Le aziende investirebbero di più e il tasso globale dell'innovazione aumenterebbe. Erodendo i ritorni sulla proprietà intellettuale, il crimine informatico disincentiva in modo invisibile l'innovazione.

Crimine finanziario senza rischi

Quando milioni di persone si vedono rubare dagli hacker le informazioni relative alla carta di credito, immediatamente l'attenzione sale. Il crimine finanziario solitamente prevede una frode, ma questa può assumere diverse forme per approfittarsi di consumatori, banche e agenzie governative. I crimini finanziari più dannosi penetrano nelle reti delle banche, con i criminali informatici che ottengono accesso ai conti e sottraggono denaro. Le rapine informatiche di alto profilo che sottraggono decine di milioni di dollari dalle banche sono un fenomeno a livello globale.

Gli esercenti sono il nuovo obiettivo dei criminali informatici. Nel 2013, una serie di attacchi che hanno causato perdite elevate hanno arricchito un elenco che include TJ Maxx, Sony e altri ancora. Si dice che gli esercenti nel Regno Unito abbiamo perso oltre 850 milioni di dollari nel 2013. Gli attacchi su larga scala hanno colpito commercianti, catene alberghiere, una linea aerea e aziende di servizi finanziari in Australia, con perdite che hanno raggiunto oltre 100 milioni di dollari per azienda. I dati personali rubati e i dati relativi alle carte di credito sono difficili da monetizzare, ma i criminali informatici stanno migliorando in questa pratica. Poiché il rischio di essere puniti è basso, questo tipo di crimine informatico andrà ad aumentare.

Informazioni aziendali riservate e manipolazione del mercato

Il furto di informazioni aziendali riservate - informazioni relative a investimenti, dati relativi a ricerche e negoziazioni commerciali sensibili - può portare un guadagno immediato. Il danno per le singole aziende ammonta a milioni di dollari. Un'azienda inglese ha segnalato ai funzionari britannici di aver perso ricavi per un ammontare di 1,3 miliardi di dollari a seguito della perdita di proprietà intellettuale con un conseguente danno per le proprie attività commerciali. La violazione di banche centrali o ministeri finanziari potrebbe fornire informazioni preziose in campo economico sull'andamento dei mercati o i tassi di interesse.

La manipolazione del mercato azionario è un'area in sviluppo per il crimine informatico. Violando le reti di un'azienda o quelle dei suoi avvocati o fiscalisti, i criminali informatici possono acquisire informazioni dall'interno su acquisizioni e fusioni pianificate, report finanziari trimestrali o altri dati che influiscono sui prezzi delle azioni di un'azienda. I criminali che si approfittano di queste informazioni a fini commerciali potrebbero essere difficili da rilevare. Gli enti normativi finanziari della Turchia, per esempio, hanno rilevato un'attività sospetta volta a manipolare i mercati e i prezzi delle azioni più sofisticata delle classiche truffe "pump and dump". Per i criminali informatici di fascia alta, le attività principali potrebbero evolversi vero la manipolazione finanziaria che sarebbe incredibilmente difficile da rilevare.

Il costo dell'opportunità

Il costo dell'opportunità è il valore delle attività ormai passate. Tre tipi di costi legati alle opportunità stabiliscono le perdite causate dal crimine informatico: investimenti ridotti in ricerca e sviluppo, comportamento avverso al rischio da parte di aziende e consumatori e una spesa maggiore per proteggere la rete. Per le aziende, il principale costo legato all'opportunità può essere rappresentato dal denaro speso per proteggere le proprie reti. Mentre le aziende spenderebbero sempre in sicurezza anche se il rischio per l'ambiente digitale fosse stato notevolmente ridotto, esiste un "rischio extra" che pagano a causa di un crimine informatico inarrestabile

Un altro modo di considerare il costo dell'opportunità del crimine informatico è vedere la perdita come una quota dell'economia di Internet. Studi stimano che l'economia di Internet generi annualmente tra i 2 e i 3 trilioni di dollari, una quota dell'economia globale che si prevede aumenterà rapidamente. Le nostre stime suggeriscono che il crimine informatico equivale al 15%-20% del valore creato da Internet, una tassa pesante per il potenziale di crescita economica e creazione di posti di lavoro.

I costi legati alla ripresa delle attività

Bonificare l'azienda dal crimine informatico è un'attività costosa. Il costo per le singole aziende legate alle attività per riprendersi dopo una frode informatica o una violazione dei dati è in crescita. Mentre i criminali non saranno in grado di monetizzare tutte le informazioni di cui si appropriano, la vittima deve spendere come se invece fosse possibile utilizzare tutti i dati rubati. Il costo aggregato per riprendere le attività a seguito di un attacco è superiore al guadagno per i criminali informatici. Uno studio sul costo del crimine informatico per l'Italia ha rilevato che mentre le perdite reali sono ammontate a solo 875 milioni di dollari, i costi legati all'opportunità e alle attività di ripresa hanno raggiunto gli 8,5 miliardi di dollari. Il conto per i costi legati alla ripresa delle attività è dove inizia il danno reale per la società e l'effetto su un'azienda può includere il danno al brand o alla reputazione e nuocere alle relazioni e alla fidelizzazione della clientela.

Incentivi e crescita costante

Gli incentivi per il crimine informatici sono classici. Il crimine informatico produce ritorni elevati a basso rischio e (relativamente) basso costo per gli hacker. Il contrario è invece vero per coloro che si difendono. Aziende e singoli prendono decisioni su come gestire la perdita potenziale causata dal crimine informatico decidendo il livello di rischio che sono disposti ad accettare e quanto desiderano spendere per ridurre tale rischio. Il problema è che se le aziende non conoscono le proprie perdite o sottostimano la loro vulnerabilità, di conseguenza sottovaluteranno il rischio.

Le opportunità per il crimine informatico aumenteranno dal momento che sempre più attività commerciali si spostano sull'online, i consumatori di tutto il mondo si collegano a Internet e dispositivi indipendenti sono collegati all'Internet delle cose. Le perdite derivanti dal furto di proprietà intellettuale aumenteranno nel momento in cui le nazioni acquirenti miglioreranno la loro capacità di utilizzare la proprietà intellettuale rubata per creare beni in concorrenza. Il crimine informatico rappresenta una tassa per l'innovazione e rallenta il passo all'innovazione globale riducendo il tasso di rendimento per coloro che innovano e per gli investitori. I governi devono avviare serie azioni sistematiche per raccogliere e pubblicare dati sul crimine informatico, per aiutare nazioni e aziende a prendere decisioni migliori relativamente a rischio e policy. Se nulla cambia, ciò che il crimine informatico riserva al mondo sono perdite maggiori e una crescita rallentata.

Informazioni su McAfee

McAfee, parte di Intel Security e società interamente controllata da Intel Corporation (NASDAQ: INTC), consente ad aziende, pubbliche amministrazioni e utenti consumer di usufruire dei vantaggi di Internet in modo sicuro. L'azienda offre prodotti e servizi di sicurezza riconosciuti e proattivi che proteggono sistemi, reti e dispositivi mobili in tutto il mondo. Grazie alla strategia Security Connected, all'approccio innovativo alla protezione rafforzata dall'hardware e all'esclusiva rete Global Threat Intelligence, McAfee è costantemente impegnata nel mantenere protetta la sua clientela. http://www.mcafee.com/it

Informazioni sul CSIS

Per 50 anni, il Center for Strategic and International Studies (CSIS) ha sviluppato soluzioni pratiche per affrontare le principali sfide mondiali. Nel celebrare questo importante traguardo, gli studiosi del CSIS continuano a fornire intuizioni strategiche e soluzioni politiche bipartisan per aiutare i responsabili delle decisioni a tracciare una rotta verso un mondo migliore.

CSIS è un'organizzazione bipartisan senza scopo di lucro con sede a Washington, DC. I 220 dipendenti a tempo pieno del Centro e la vasta rete di studiosi affiliati conducono ricerche e analisi e sviluppano iniziative politiche che guardano al futuro e anticipano il cambiamento. http://csis.org/

McAfee Srl
Via Fantoli 7
20138 Milano
Italia
(+39) 02.554171
www.mcafee.com/it

61080rps_csis-econ-cybercrime-sum_fnl_0514