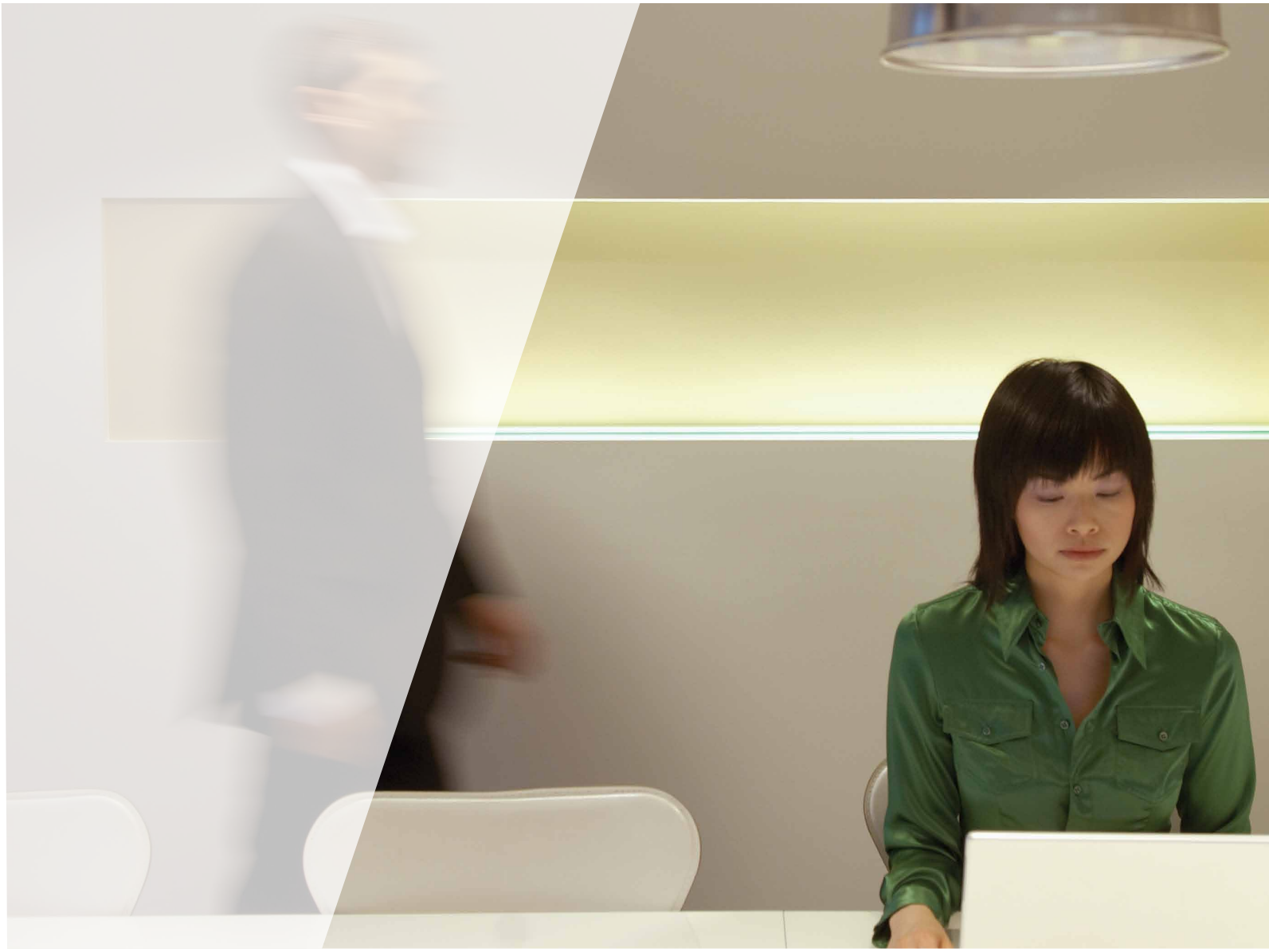
Nel mirino

Le infrastrutture critiche nell'era della guerra informatica

Report globale sulle minacce per le industrie strategiche



Nel mirino

Autori:

Stewart Baker, distinguished visiting fellow, CSIS; partner, Steptoe & Johnson

Shaun Waterman, scrittore e ricercatore, CSIS

George Ivanov, ricercatore, CSIS

INDICE DEI CONTENUTI

Introduzione e informazioni generali sullo studio

In un mondo sempre più interconnesso, le vulnerabilità informatiche delle infrastrutture critiche pongono una serie di sfide a governi, proprietari e gestori di tutti i settori in tutto il mondo.

Con l'economia mondiale ancora instabile dopo la crisi finanziaria dell'ultimo anno, l'integrità e la disponibilità delle industrie nazionali strategiche potrebbero diventare meno prioritarie per i governi, ma continuano comunque a rappresentare un fattore determinante a livello di vulnerabilità strategica.

600 dirigenti responsabili dell'IT e della sicurezza delle infrastrutture critiche di sette settori, distribuite in 14 paesi di tutto il mondo, hanno risposto in maniera anonima a una lunga serie di domande dettagliate su procedure, atteggiamenti e policy in materia di sicurezza, impatto delle normative, rapporto con il governo, misure di sicurezza specifiche implementate nelle loro reti e tipi di attacchi che si trovano ad affrontare.

I proprietari e i gestori di infrastrutture critiche riferiscono che le loro reti IT vengono ripetutamente colpite da attacchi informatici, spesso lanciati da avversari di alto livello. In molti casi questi attacchi hanno un impatto estremamente grave, con costi elevati e diffusi.

Anche se in genere i dirigenti si dichiarano soddisfatti delle risorse di cui dispongono per la sicurezza, i tagli causati dalla recessione sono stati generalizzati e spesso consistenti. Esiste inoltre una certa incertezza sulla capacità delle infrastrutture critiche di far fronte ad attacchi su larga scala.

Raccogliendo informazioni sulle misure di sicurezza effettivamente adottate dalle aziende abbiamo potuto effettuare un confronto oggettivo della sicurezza tra i vari settori di infrastrutture critiche e le varie nazioni. Ai dirigenti con responsabilità a livello di sistemi di controllo operativi o industriali è stata posta anche una serie di domande specifiche sulle misure di sicurezza impiegate per questi sistemi.

I dirigenti cinesi sono quelli che hanno riferito i più alti tassi di adozione delle misure di sicurezza, comprese la crittografia e l'autenticazione avanzata degli utenti. Fra i vari settori, il tasso di adozione più basso è stato riferito dai dirigenti del settore idrico/fognario.

Suddivisi per settore e nazione, i dati dell'indagine indicano notevoli variazioni nell'atteggiamento e nei resoconti relativi alle normative e ad altri interventi governativi. I livelli di regolamentazione più elevati sono stati segnalati per l'India, seguita da vicino da Cina e Germania. I dirigenti statunitensi hanno riferito i livelli più bassi. Le opinioni sull'impatto e sull'efficacia delle normative si sono rivelate estremamente discordi, ma nel complesso la maggior parte degli intervistati concordava sul fatto che le normative consentono di migliorare la sicurezza.

La maggior parte dei dirigenti riteneva che i governi stranieri fossero già coinvolti negli attacchi alle reti delle infrastrutture critiche del loro paese. Stati Uniti e Cina erano visti come i più temibili aggressori potenziali, ma le difficoltà legate all'attribuzione delle responsabilità nel cyberspazio consentono a tutti gli aggressori di ricorrere all'espediente della "negazione plausibile".

Metodologia

I dati raccolti per questo report forniscono per la prima volta un quadro dettagliato del modo in cui i responsabili della difesa delle reti IT critiche rispondono agli attacchi informatici, cercando di proteggere i propri sistemi e collaborando con i governi. Un team del programma per le tecnologie e le politiche pubbliche del CSIS (Center for Strategic and International Studies) di Washington ha analizzato i dati, li ha integrati con ricerche e interviste aggiuntive e ha redatto questo report.

Gli intervistati sono dirigenti con responsabilità a livello di IT, sicurezza o sistemi di controllo operativo all'interno della propria azienda. Circa la metà ha dichiarato di avere responsabilità a livello di business unit, un quarto a livello mondiale.

L'indagine non è stata concepita come sondaggio di opinione statisticamente valido con margini di campionamento ed errore. Si tratta piuttosto di un'indicazione di massima dell'opinione dei dirigenti, un'istantanea del punto di vista di un gruppo significativo di responsabili delle decisioni aziendali[1].

Il team del CSIS ha utilizzato le interviste per fornire un contesto, informazioni generali e un riscontro per i dati dell'indagine, discutendo le best practice adottate e aggiungendo ulteriori dettagli al quadro degli ambienti normativi e dei livelli di minaccia/vulnerabilità nei sette settori esaminati in ogni paese. Molti intervistati non hanno acconsentito a essere citati per nome; alcuni hanno chiesto di non essere citati del tutto. Tutti quelli che hanno accettato di essere identificati sono menzionati nei ringraziamenti.


La minaccia è reale
BUS

Le reti e i sistemi di controllo vengono ripetutamente colpiti da attacchi informatici, spesso lanciati da avversari di alto livello come gli stati-nazione stranieri.

I proprietari e i gestori di infrastrutture critiche riferiscono che le loro reti e i loro sistemi di controllo vengono ripetutamente colpiti da attacchi informatici, spesso lanciati da avversari di alto livello come gli stati-nazione stranieri. Si va da massicci attacchi DDoS (Distributed Denial-of-Service) concepiti per mettere fuori uso i sistemi fino a tentativi occulti di penetrare nelle reti senza essere individuati.

Anche se l'attribuzione delle responsabilità è estremamente difficile nel caso degli attacchi informatici, la maggior parte dei proprietari e dei gestori ritiene che i governi stranieri siano già coinvolti negli attacchi alle infrastrutture critiche del loro paese. Gli altri aggressori vanno da semplici vandali a gruppi di criminali organizzati. Gli attacchi motivati da interessi economici, come l'estorsione e il furto di servizi, sono molto diffusi.

L'impatto degli attacchi informatici varia enormemente, ma in alcuni casi sono state registrate conseguenze molto gravi, ad esempio l'interruzione di attività operative critiche. Il costo del downtime causato dagli attacchi di grandi proporzioni supera i 6 milioni di dollari al giorno. A parte i costi, la conseguenza più temuta in caso di attacco è il danno per la reputazione, seguito dalla perdita di informazioni personali dei clienti.

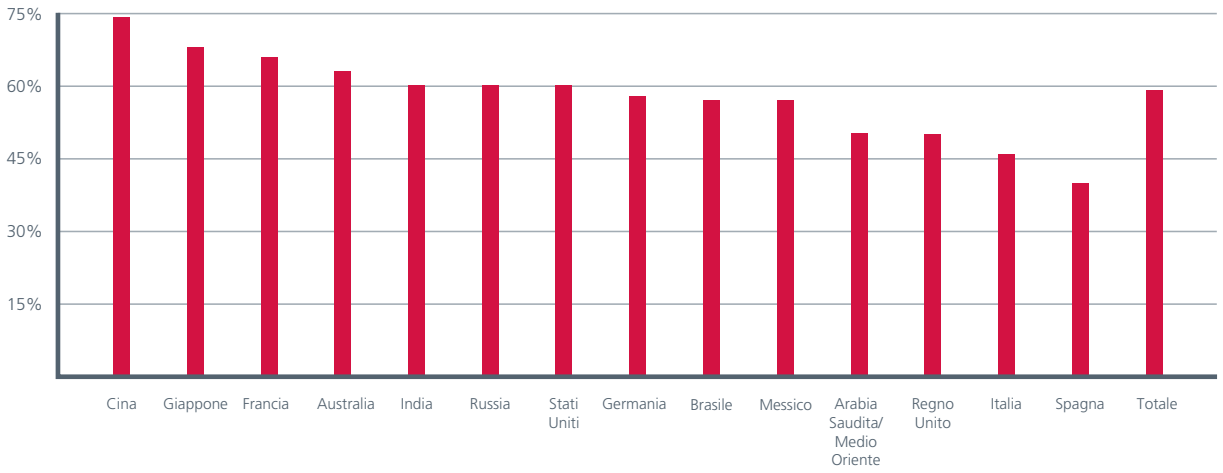
Per quanto inquietante possa essere questo scenario, gli intervistati ritengono che in futuro la situazione potrà solo peggiorare.

Gli attacchi critici sono sempre più diffusi

Oltre la metà dei dirigenti interpellati (54%) ha dichiarato di aver subito "attacchi DoS (denial of service) su larga scala da parte di avversari di alto livello come organizzazioni criminali, terroristi o stati-nazione (come è avvenuto ad esempio in Estonia e in Georgia)". La stessa percentuale ha affermato di aver subito "infiltrazioni occulte" da parte di questi avversari di alto livello, "ad esempio GhostNet", una rete di spionaggio su larga scala che, grazie ad attacchi malware mirati, ha consentito agli hacker di violare, controllare e scaricare grandi quantità di dati dalle reti informatiche di organizzazioni no profit, dipartimenti governativi e organizzazioni internazionali in decine di paesi.

Una cospicua maggioranza (59%) riteneva che rappresentanti di governi stranieri fossero già coinvolti in questo tipo di infiltrazioni e attacchi rivolti alle infrastrutture critiche dei loro paesi.

Percentuale di intervistati secondo cui governi stranieri sono stati coinvolti negli attacchi informatici alle infrastrutture critiche del loro paese



La maggioranza ritiene che i governi stranieri siano già coinvolti negli attacchi informatici alle infrastrutture critiche.

Nel 2007, il Report McAfee sulla criminologia virtuale ha concluso che 120 paesi possedevano, o stavano sviluppando, capacità di spionaggio informatico o guerra informatica. Le autorità di Regno Unito e Germania hanno comunicato alle industrie critiche del settore privato che le loro reti erano oggetto di intrusioni da parte di servizi di intelligence stranieri. Negli Stati Uniti la stampa ha dato ampio risalto alle intrusioni da parte di agenzie di intelligence straniere, spesso attribuite alla Cina e dirette in particolare al settore dell'energia e della produzione per la difesa.

"Esistono sicuramente entità straniere che mirano a effettuare un monitoraggio (informatico) delle nostre infrastrutture energetiche", ha affermato Michael Assante, chief security officer della North American Electric Reliability Corporation (NERC). "L'obiettivo è di acquisire conoscenze, creare le condizioni necessarie per infiltrarsi e cercare di garantirsi un accesso permanente alle reti informatiche".

Gli attacchi sono frequenti e hanno un forte impatto

Quasi un terzo degli intervistati (29%) ha riferito di aver subito più attacchi DDoS (Distributed Denial-of-Service) su larga scala ogni mese, e quasi due terzi di essi (64%) hanno affermato che questi attacchi hanno "avuto un impatto sulle attività operative".

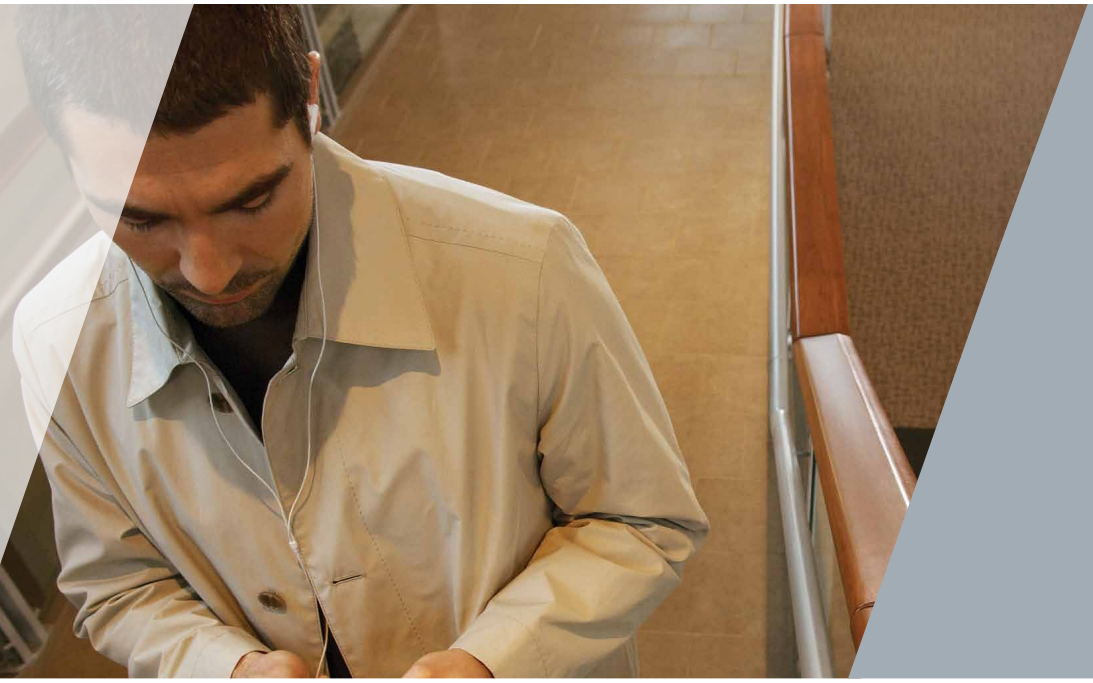
Gli attacchi DDoS sfruttano reti di computer infetti, spesso appartenenti a singoli o aziende che non sanno neppure di essere stati colpiti, per bombardare altre reti con milioni di richieste di informazioni fasulle trasmesse via Internet. Gli attacchi DDoS vengono lanciati da "botnet" (ovvero "reti di robot") di computer che sono stati infettati da software dannoso appositamente sviluppato, il cosiddetto malware.

Negli ambienti di rete odierni gli attacchi DDoS sono tecnicamente più semplici da rilevare e neutralizzare, e la maggior parte degli Internet Service Provider (ISP) offre servizi di mitigazione, a pagamento, ai propri clienti.

"Molti ISP ritengono che il nostro compito sia semplicemente di veicolare il traffico", ha affermato Adam Rice, chief security officer di Tata Communications, il più grande fornitore mondiale di servizi Internet. "Se paghi per il servizio (di mitigazione), bloccheranno gli attacchi DDoS prima che arrivino a te; in caso contrario i provider tendono a disinteressarsi del problema".

Attraverso un'azione congiunta, ha commentato, i "provider di primo livello", ovvero quelli che possiedono e gestiscono le dorsali della rete Internet globale, potrebbero fare molto di più dal punto di vista tecnico per mitigare tali attacchi.

Il problema, come hanno osservato altri esperti, è che queste attività di mitigazione potrebbero essere complicate da questioni di natura normativa e contrattuale, a meno che la legge non garantisca meccanismi di protezione Safe Harbor alle aziende che intercettano e deviano il traffico DDoS. Inoltre, i provider che operano in più mercati nazionali potrebbero trovarsi a gestire obblighi legali differenti o addirittura contrastanti nelle varie giurisdizioni.



Quasi due terzi degli intervistati che hanno subito attacchi DDoS su larga scala hanno affermato che le loro attività operative hanno subito un impatto.

Gli autori degli attacchi sono spesso anonimi

Le istruzioni di attacco trasmesse alle botnet provengono spesso da altri computer infetti, a loro volta di proprietà di terzi inconsapevoli, mentre i veri autori rimangono nascosti grazie a scappatoie e depistaggi. Le botnet possono essere facilmente prese in affitto da bande di hacker. Questi fattori possono rendere molto difficile l'individuazione della vera origine degli attacchi DDoS. La reale identità degli autori degli attacchi sferrati contro Georgia ed Estonia rimane tuttora controversa.

"Essere a conoscenza di un fatto e poterlo dimostrare sono due cose diverse", ha affermato un ex funzionario delle forze dell'ordine statunitensi. "Anche se riesci a risalire a un computer specifico, non è detto che tu sappia chi l'ha utilizzato".

Lo stesso principio vale a maggior ragione per le infiltrazioni occulte nelle reti. Nel caso di GhostNet, i ricercatori hanno rilevato la presenza di spyware (software progettato per sottrarre password, dati di accesso e documenti riservati) nelle reti informatiche dell'ufficio del leader spirituale tibetano, il Dalai Lama, e hanno accusato il governo cinese. L'attribuzione delle responsabilità non era basata esclusivamente su riscontri tecnici, ma anche sul fatto che i dati sottratti dalle reti compromesse sono stati in seguito utilizzati da funzionari cinesi.

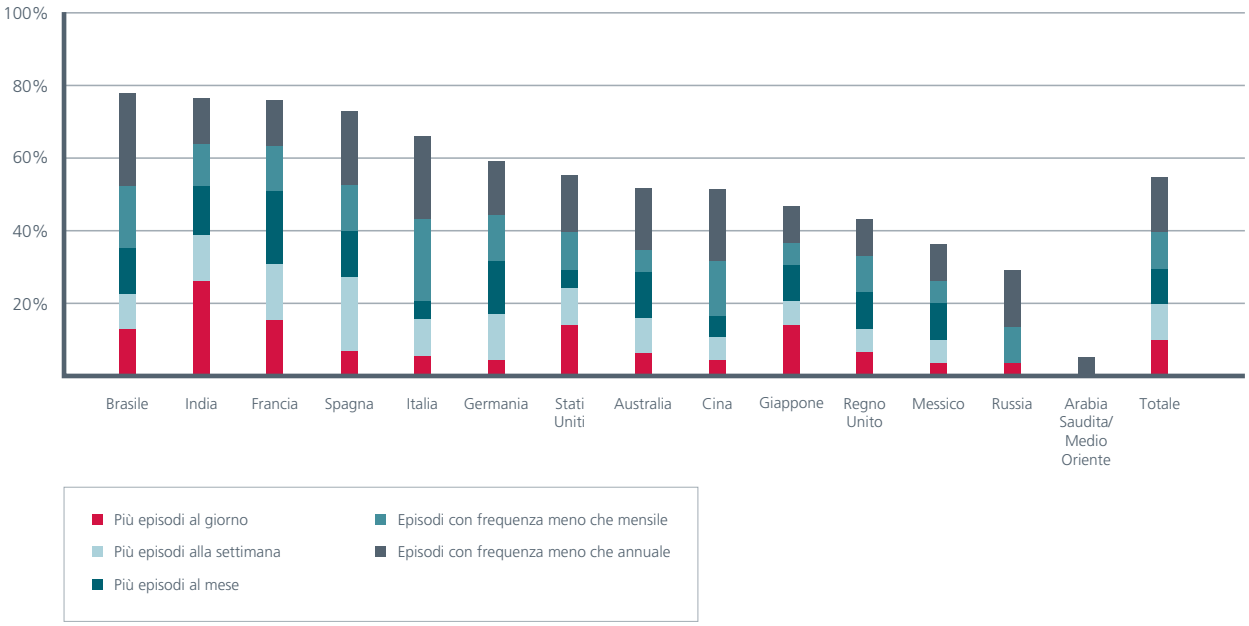
Poiché attribuire con precisione le responsabilità degli attacchi informatici è estremamente difficile, gli stati-nazione coinvolti continuano a sfruttare i vantaggi strategici della "negazione plausibile". Ma i responsabili della protezione delle reti critiche potrebbero avere una visione hobbesiana del conflitto informatico e considerarlo una "guerra di tutti contro tutti".

Gli attacchi DDoS, benché diffusi, non sono il problema più ricorrente per la sicurezza

La forma di attacco più diffusa è l'infezione da virus o malware, subita dall'89% degli intervistati. Ma sono stati registrati tassi di incidenza superiori al 70% anche per una vasta gamma di attacchi di altro tipo, ad esempio episodi di vandalismo e attacchi DDoS di basso livello, minacce provenienti da soggetti interni all'azienda, fughe o fuoriuscite di dati sensibili, phishing e pharming.

Gli attacchi tecnicamente più sofisticati sono stati più rari, anche se hanno avuto una diffusione comunque maggiore rispetto agli attacchi DDoS su larga scala. Più della metà dei dirigenti IT (57%) ha riferito casi di DNS poisoning (reindirizzamento del traffico web) e quasi la metà di loro ha affermato di aver subito più episodi in un mese. Circa la stessa percentuale è stata colpita da attacchi con iniezione SQL, che vengono utilizzati dagli hacker per ottenere l'accesso ai dati back-end attraverso un sito web pubblico, e anche in questo caso quasi la metà ha subito più attacchi mensili. Gli attacchi di questo tipo, inoltre, hanno avuto un impatto operativo più rilevante sui sistemi colpiti.

Percentuale che ha riferito attacchi DDoS su larga scala e frequenza degli attacchi



Il furto e altri moventi economici hanno una forte incidenza

Il 60% degli intervistati ha riferito episodi di furto di servizi; quasi uno su tre ha subito più attacchi di questo tipo ogni mese. I tassi di incidenza più alti sono stati registrati nel settore gaspetrolifero, dove i furti di servizi hanno colpito tre quarti degli interpellati. Questo settore ha registrato anche i più alti tassi di infiltrazioni occulte (71% rispetto al 54% del totale degli intervistati) e più di un terzo ha subito più infiltrazioni ogni mese.

In generale, tuttavia, le variazioni dei tassi di incidenza sono risultate maggiori tra un paese e l'altro anziché tra un settore e l'altro. Questo dato fa pensare che i fattori nazionali siano più significativi di quelli settoriali nella determinazione dei tassi di attacco.

Alcuni paesi subiscono più attacchi informatici di altri

In India e in Francia oltre la metà dei dirigenti ha subito più attacchi DDoS su larga scala ogni mese. Anche Spagna e Brasile hanno registrato tassi di incidenza elevati con più episodi mensili[2].

"Gli attacchi DDoS sono molto comuni in Brasile, e lo stesso si può dire del resto del mondo", ha affermato l'analista di iDefense Labs Achises De Paula, che ha aggiunto che gli ISP hanno iniziato ad adottare metodi più efficaci per gestire gli attacchi di questo tipo.

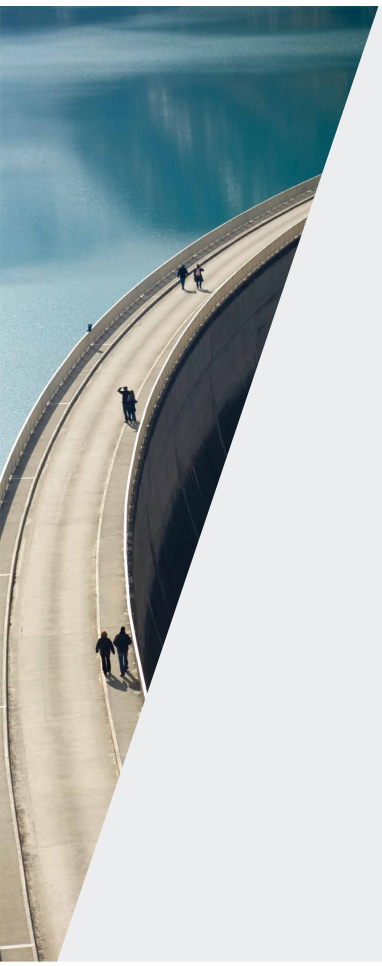
"La popolarità degli attacchi DDoS è in costante aumento. Costano sempre meno e diventano sempre più facili da attuare", ha commentato Rice. "Per lanciare un attacco DDoS puoi affittare una botnet, usando la carta di credito, nel giro di due ore".

Gli attacchi DDoS colpiscono tutti i settori

Le variazioni settoriali degli attacchi DDoS su larga scala sono state molto inferiori rispetto alle variazioni tra un paese e l'altro, un dato che probabilmente indica una maggiore rilevanza dei fattori nazionali rispetto a quelli settoriali nella determinazione dei tassi di incidenza. Il settore più colpito è stato quello gaspetrolifero: due terzi dei dirigenti hanno affermato di aver subito attacchi di questo tipo e un terzo di loro ha subito più attacchi ogni mese. I settori meno colpiti sono stati quello idrico/fognario, con una percentuale del 43%, e quello dei trasporti (50%).

Gli attacchi hanno un forte impatto che varia da un settore all'altro

Quasi due terzi degli intervistati che hanno subito attacchi DDoS su larga scala hanno affermato che questi attacchi hanno avuto un impatto sulle attività operative. Oltre a rendere inaccessibili i siti web pubblici, gli attacchi di questo tipo possono compromettere la connettività e-mail, i sistemi telefonici basati su Internet e altre funzioni importanti dal punto di vista operativo.



Estorsione via web

Negli ultimi due anni un'infrastruttura critica su cinque ha subito un'estorsione perpetrata mediante un attacco informatico reale o minacciato. Questo dato sconcertante è in linea con gli episodi riferiti dagli esperti di vari paesi e settori. In realtà, alcuni di loro ritengono che la cifra reale potrebbe essere addirittura superiore. Nella maggior parte dei casi le aziende colpite preferiscono non dare risonanza a questi episodi, o li tengono addirittura segreti, perché temono un danno per la reputazione o conseguenze di altro tipo.

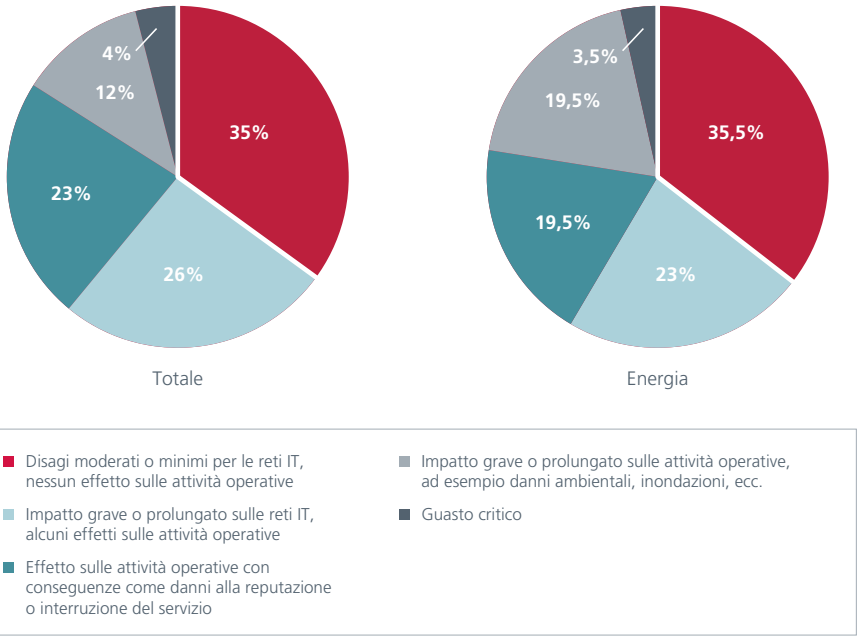
I tassi di incidenza più alti sono stati registrati nel settore energetico (27%) e in quello gaspetrolifero (31%).

"Il fenomeno dell'estorsione mi preoccupa soprattutto in relazione all'interruzione della fornitura energetica", ha commentato Assante. Assante ritiene che le minacce alle reti aziendali rappresentino una forma di estorsione "di livello più basso", "il modo più sicuro per estorcere denaro in maniera occulta a un livello non materiale". Le minacce alle infrastrutture vere e proprie sono molto più gravi. "Se hai di fronte un avversario che è in grado di 'staccare la spina', il quadro cambia completamente. Probabilmente l'estorsore corre un rischio molto maggiore, ma può anche avanzare richieste economiche molto superiori". Nel novembre del 2009 i media statunitensi hanno riferito che due blackout avvenuti in Brasile nel 2005 e nel 2007 erano stati causati dagli hacker, probabilmente nell'ambito di un piano estorsivo.

Nel settembre del 2009 Mario Azer, consulente IT della società di esplorazione gaspetrolifera Pacific Energy Resources di Long Beach, California, ha confessato di aver sabotato i sistemi informatici dell'azienda in seguito a una controversia sulle sue prospettive future di lavoro e retribuzione. La manomissione riguardava in particolare il software di controllo industriale denominato SCADA (Supervisory Control And Data Acquisition), un sistema che in questo caso serviva a segnalare agli operatori eventuali perdite o danni alle condutture sottomarine che collegano le torri di trivellazione della società alla terraferma.

Anche se il settore idrico/fognario ha registrato un tasso di incidenza inferiore (17%), il potenziale impatto dei piani estorsivi è comunque molto sentito in questo campo.

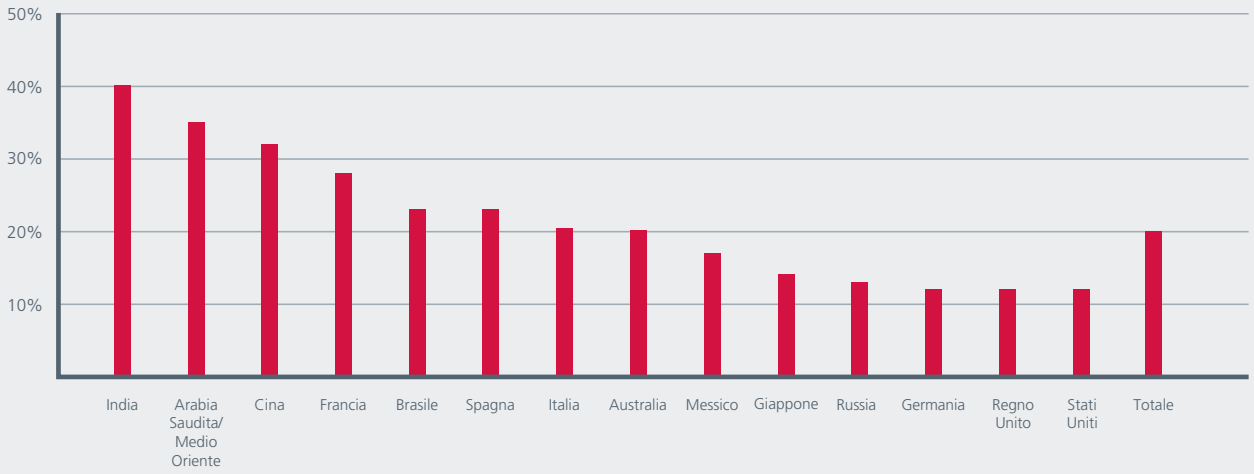
Impatto degli attacchi DDoS su larga scala



"L'acqua potabile è un bene che la maggior parte degli americani e dei suoi leader politici dà per scontato da almeno un secolo a questa parte", ha affermato Aaron Levy della Association of Metropolitan Water Agencies. "Una perdita di fiducia nel sistema di fornitura dell'acqua potabile, hanno indicato gli studi, potrebbe generare una situazione di caos" nelle principali città e negli altri centri abitati.

I tassi di estorsione più elevati sono stati registrati in India, Arabia Saudita/Medio Oriente, Cina e Francia; quelli più bassi nel Regno Unito e negli Stati Uniti.

Percentuale di estorsioni perpetrate mediante un attacco di rete reale o minacciato negli ultimi due anni



Circa uno su sei ha descritto l'impatto degli attacchi DDoS su larga scala come "effetti gravi o prolungati sulle attività operative" o come "guasto critico".

Questi attacchi DDoS su larga scala hanno avuto un effetto particolarmente dannoso nel settore energetico e in quello idrico/fognario.

Gli altri tipi di attacchi che hanno avuto un forte impatto a livello operativo sono stati le infiltrazioni occulte nelle reti, le fughe o fuoriuscite di dati sensibili, il DNS poisoning e le iniezioni SQL, che hanno avuto conseguenze operative per oltre il 60% delle vittime. Nel caso delle fughe o fuoriuscite di dati sensibili, il 15% ha affermato che l'impatto è stato grave e il 4% lo ha definito critico.

I dirigenti hanno parlato anche degli altri effetti degli attacchi informatici. A livello non operativo, la conseguenza più temuta è il danno per la reputazione, seguito dalla divulgazione delle informazioni personali dei clienti. Questi due problemi sono particolarmente sentiti nel settore bancario.

Il movente economico

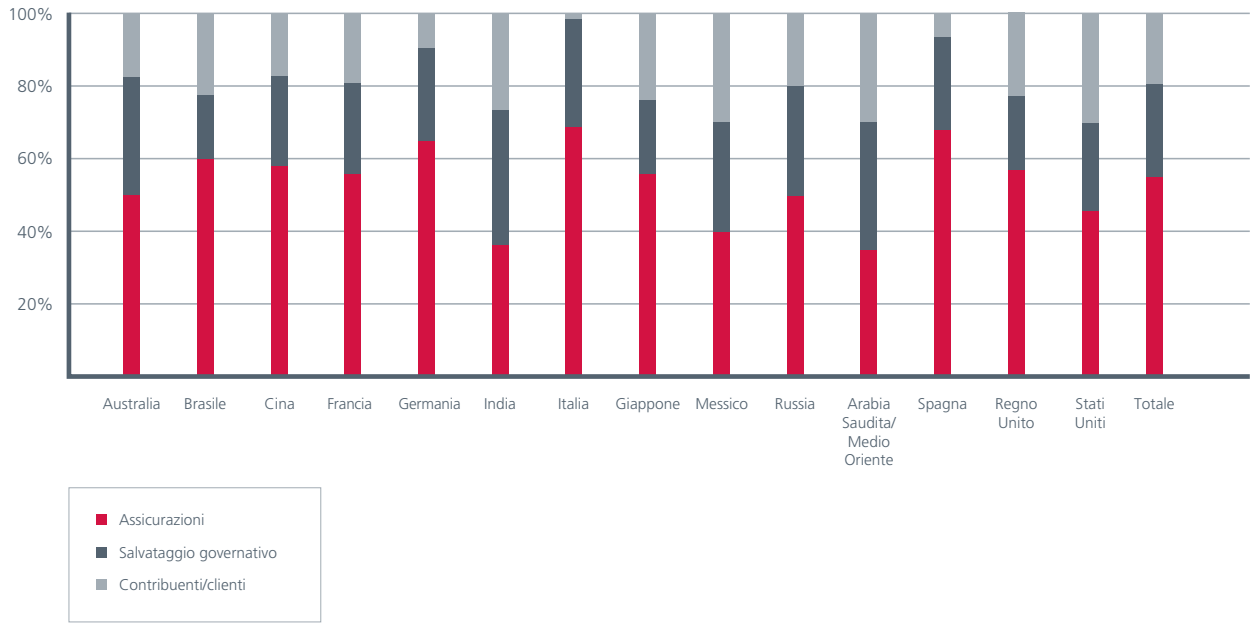
Quando è stato chiesto di indicare l'obiettivo più comune degli attacchi informatici, più della metà degli intervistati (56%) ha menzionato le informazioni finanziarie. Gli obiettivi meno frequenti sono stati password e informazioni di accesso, colpite solo nel 21% dei casi.

Nel settore energetico e in quello gaspetrolifero, tuttavia, gli attacchi hanno riguardato principalmente i sistemi di controllo operativo computerizzati come SCADA, colpiti rispettivamente nel 55% e nel 56% dei casi in questi due settori.

I sistemi di controllo operativo sono sotto attacco

Gli attacchi ai sistemi SCADA sono particolarmente insidiosi perché consentono agli hacker di assumere il controllo diretto dei sistemi operativi, aprendo potenzialmente la strada a blackout di vaste proporzioni o disastri ambientali dolosi.
(vedere pagina 22)

Chi sosterrebbe i costi di un incidente informatico di grandi proporzioni



Nel 2007 la CNN ha acquisito il video di un test condotto dagli scienziati dell'Idaho National Laboratory. Il video mostrava un generatore elettrico, collegato a un sistema SCADA, che vibrava fino quasi a ridursi in pezzi dopo aver ricevuto istruzioni manipolate. Il video metteva in evidenza il problema delle vulnerabilità SCADA negli Stati Uniti e ha dato il via ad audizioni del Congresso sulla sicurezza informatica della rete elettrica.

Gli attacchi informatici di grandi proporzioni hanno costi elevati

I dati dell'indagine indicano che i costi del downtime causato da un incidente di sicurezza informatica di grandi proporzioni ("ad esempio un incidente che causa un'interruzione grave dei servizi per almeno 24 ore, la perdita di vite umane, lesioni personali o il fallimento di una società") sarebbero molto alti.

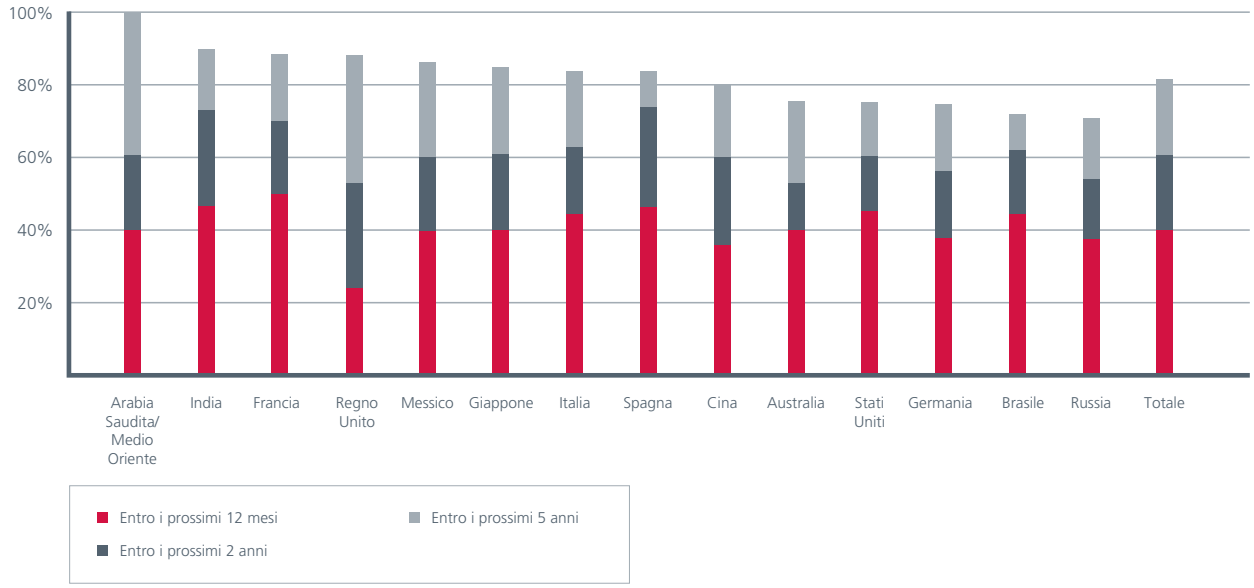
In media, gli intervistati hanno stimato che 24 ore di downtime a seguito di un attacco grave costerebbero alla loro azienda 6,3 milioni di dollari. I costi più alti sono stati indicati nel settore gaspetrolifero, dove la stima media è stata di 8,4 milioni di dollari al giorno. Le stime più basse sono state fornite per il settore governativo e quello idrico/fognario.

Chi paga?

Sono state registrate opinioni molto discordi su chi debba sostenere questi costi in ultima analisi. Più della metà degli intervistati riteneva che i costi sarebbero stati coperti dalle assicurazioni, quasi uno su cinque ha affermato che i costi ricadrebbero su utenti e clienti e solo poco più di un quarto si aspettava un intervento del governo. La convinzione che i costi verrebbero sostenuti dalle assicurazioni ha registrato le percentuali più alte in Italia, Spagna e Germania e quelle più basse in India e Arabia Saudita.

La percentuale di intervistati secondo cui i costi sarebbero a carico dei clienti è risultata quasi doppia nel settore idrico/fognario rispetto al totale degli intervistati (35% contro 19%). Nei casi in cui le risposte del settore idrico si discostano notevolmente dai risultati generali, tuttavia, è opportuno ricordare che in questo settore è stato intervistato un campione ridotto di persone. Ma l'idea che a pagare sarebbero i clienti era diffusa anche nel settore dei trasporti (24%) e delle telecomunicazioni (23%). La percentuale più bassa è stata registrata nel settore gaspetrolifero (12%).

Entro quanto tempo è previsto un incidente informatico di grandi proporzioni nelle infrastrutture critiche del paese



Il costo stimato medio di 24 ore di downtime a seguito di un attacco informatico grave sarebbe di 6,3 milioni di dollari.

Queste aspettative potrebbero rivelarsi ottimistiche. In futuro, suggerisce un esperto, è probabile che cambino perché le aziende cercheranno di limitare le proprie responsabilità di fronte ai crescenti costi degli attacchi informatici.

"Finora i consumatori australiani sono stati fortunati: il problema riguardava sempre qualcun altro", ha affermato Ajoy Ghosh, security executive di Logica con sede a Sydney. "Se sono un privato e rimango vittima di un attacco di phishing… so che la banca mi rimborserà… Prevedo che in futuro la situazione verrà ribaltata e dovrò farmi carico del problema in prima persona".

Secondo Ghosh, docente di cybercrime presso la University of Technology di Sydney, le aziende che cercano di limitare le proprie responsabilità "possono unicamente scaricare il problema su qualcun altro. In alcuni casi si tratterà del governo, in altri dell'assicurazione. Ma nella maggior parte dei casi, a mio avviso, quel qualcun altro sarà il consumatore".

Il rischio di attacchi informatici è in aumento

La situazione sta peggiorando. Il numero di intervistati secondo cui la vulnerabilità agli attacchi informatici del proprio settore è aumentata nell'ultimo anno è risultato quasi doppio rispetto al numero di coloro che hanno affermato che è diminuita (37% contro 21%).

È opportuno sottolineare che due quinti di questi dirigenti IT hanno dichiarato di aspettarsi un incidente di sicurezza informatica di grandi proporzioni (un incidente che causa un'interruzione per "almeno 24 ore, la perdita di vite umane… o il fallimento di una società") nel proprio settore entro il prossimo anno. Ad eccezione del 20%, tutti si aspettavano un incidente di questo tipo entro cinque anni. Questa visione pessimistica era particolarmente accentuata nei paesi che stanno già sperimentando i più alti livelli di attacchi critici.

Rispondere alla minaccia: risorse e livello di preparazione

I tagli alle risorse di sicurezza causati dalla recessione sono generalizzati. Perorare la causa della sicurezza informatica rimane un compito impegnativo.

La maggior parte dei dirigenti IT dichiara di disporre di risorse adeguate per la protezione della rete, anche se il livello di soddisfazione varia considerevolmente da un paese all'altro. Ma le attuali condizioni economiche hanno determinato tagli generalizzati a queste risorse. Perorare la causa della sicurezza informatica rimane un compito molto impegnativo.

La fiducia nelle risorse disponibili non corrisponde sempre a un'analoga fiducia nel proprio livello di preparazione. Circa un terzo degli intervistati ha affermato che il proprio settore non è pronto a gestire attacchi di grandi proporzioni o infiltrazioni occulte da parte di avversari di alto livello. Gli europei, in particolare, hanno scarsa fiducia nella capacità delle loro infrastrutture bancarie di continuare a operare in caso di attacco informatico critico.

Le risorse sono generalmente considerate adeguate

In genere i dirigenti IT hanno dichiarato di disporre di risorse adeguate per la protezione delle reti informatiche della propria azienda. Quasi due terzi degli intervistati hanno affermato che le proprie risorse erano "totalmente" o "sostanzialmente" adeguate. Solo poco più di un terzo ha dichiarato che le risorse erano "inadeguate" o "piuttosto inadeguate".

Alcuni paesi e settori erano meno soddisfatti di altri

Il tasso di soddisfazione più basso è stato registrato in Italia, Giappone e Arabia Saudita; il più alto in Germania, nel Regno Unito e in Australia. I dirigenti del settore bancario sono stati quelli che si sono dichiarati in generale più soddisfatti; i meno soddisfatti appartenevano al settore dei trasporti.

I tagli alle risorse causati dalla recessione sono generalizzati e in alcuni casi consistenti

Due terzi dei dirigenti IT intervistati hanno dichiarato che le risorse di sicurezza a loro disposizione erano state tagliate a causa della recessione.

Uno su quattro ha affermato che i tagli avevano ridotto le risorse di almeno il 15%. I tagli più diffusi hanno riguardato il settore energetico e quello gaspetrolifero, settori in cui fino a tre quarti degli intervistati hanno riferito riduzioni delle risorse. La percentuale di tagli più alta è stata registrata in India, Spagna, Francia e Messico; la più bassa in Australia.

La sicurezza è un fattore chiave nelle decisioni sugli investimenti

Anche in un periodo di recessione, la sicurezza rimane il principale fattore trainante per le decisioni in materia di policy e investimenti IT. Per le decisioni in materia di policy e investimenti IT, il 92% ha affermato che la sicurezza ha rappresentato un fattore "fondamentale" o "molto importante". Una percentuale molto simile, il 91%, ha espresso lo stesso giudizio sull'affidabilità. Gli altri due fattori presi in considerazione nell'indagine, efficienza e disponibilità, sono stati definiti fondamentali o molto importanti da tre quarti dei dirigenti.

La sicurezza è stata definita "fondamentale" soprattutto dai dirigenti cinesi e statunitensi.

Incentivi aziendali per la sicurezza informatica: lo sgabello a tre gambe

Nel complesso, il fattore citato più frequentemente come "principale ostacolo al raggiungimento della sicurezza delle reti critiche" sono stati i costi, seguiti dalla "mancanza di consapevolezza della portata del rischio".

Nel settore idrico/fognario e in quello gaspetrolifero, tuttavia, è stata registrata una tendenza opposta: la mancanza di consapevolezza è stata menzionata più frequentemente dei costi. Gli specialisti di sicurezza di vari settori hanno affermato che perorare la causa della sicurezza informatica rimane un compito molto impegnativo perché il management spesso non comprende la portata della minaccia o i requisiti delle soluzioni da adottare.

"Credo che l'ostacolo principale sia il fatto che gli addetti alla sicurezza non sono stati in grado di comunicare efficacemente l'urgenza del problema e non sono riusciti a convincere i responsabili delle decisioni della concretezza della minaccia", ha affermato uno specialista di sicurezza. Ha inoltre aggiunto che il problema è in parte dovuto al fatto che la sicurezza non è ancora diventata un differenziatore di mercato significativo per le industrie critiche.

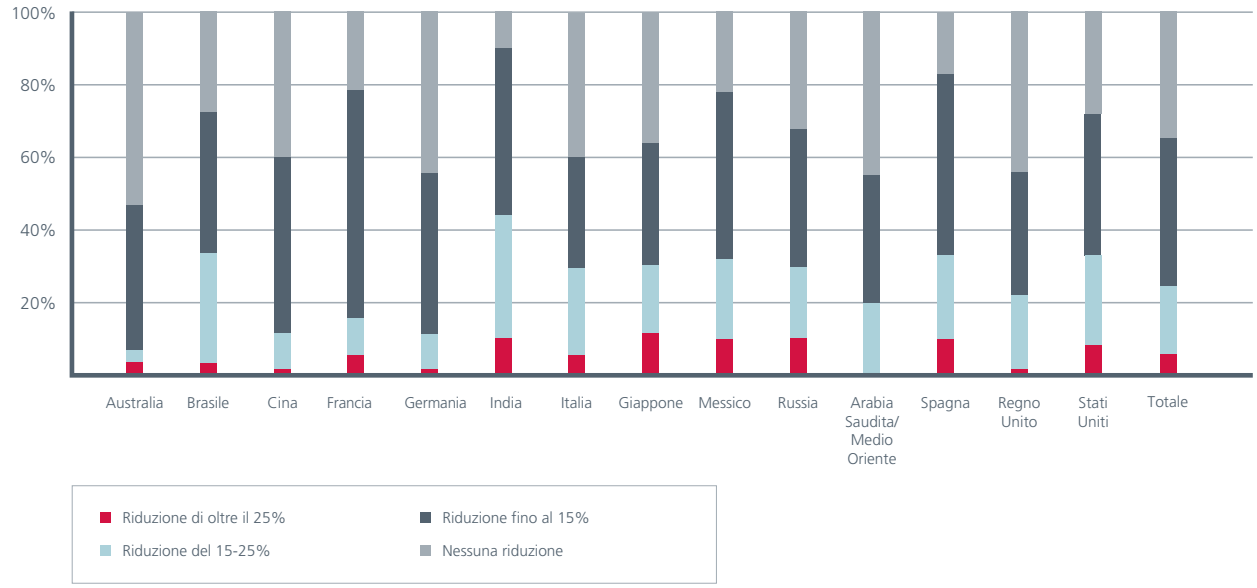
Il parere comune degli esperti era che la consapevolezza dei problemi relativi alla sicurezza informatica fosse aumentata negli Stati Uniti e in altri paesi dopo gli attacchi terroristici dell'11 settembre, con un'attenzione crescente da parte dei governi al rafforzamento delle infrastrutture critiche. Allo stesso tempo, tuttavia, gli esperti ritenevano che la strada da percorrere fosse ancora lunga.

"La sicurezza informatica ha iniziato solo di recente ad attirare l'attenzione dei manager e dei responsabili della sicurezza delle aziende di pubblica utilità", ha affermato Aaron Levy della Association of Metropolitan Water Agencies. "Stanno cercando tutti di recuperare il tempo perso", ha aggiunto uno specialista del settore dei trasporti.

Sfortunatamente, la migliore maestra continua a essere l'esperienza. In altre parole, spesso è necessario subire un attacco critico per convincere il management della concretezza della minaccia e della necessità di proteggersi. "In genere, le aziende che gestiscono la sicurezza informatica in maniera efficace sono quelle che hanno subito almeno un incidente in passato", ha commentato lo specialista.

D'altra parte, secondo il chief security officer di uno dei principali fornitori mondiali di servizi di telecomunicazioni e Internet, i clienti hanno iniziato a prestare attenzione alla sicurezza,

Tagli alle risorse di sicurezza causati dalla recessione



trasformandola in un differenziatore di mercato. "Dipende tutto dai clienti", ha affermato Adam Rice di Tata. "Non succede più che il cliente arrivi alla fase di stipulazione del contratto e chieda distrattamente 'oh, a proposito, cosa mi offrite a livello di sicurezza?' La domanda viene posta subito, si tratta di un requisito assoluto… i nostri clienti chiedono prove tangibili. Vogliono organizzare conference call e porci domande spinose, vogliono visitare i data center, avere la possibilità di accedere alle nostre sedi senza preavviso… i clienti ci fanno l'elenco dei requisiti e noi abbiamo l'obbligo di rispettarli".

Nonostante questo, perorare la causa della sicurezza può essere un compito molto impegnativo. "Nessuno vuole pagare il premio dell'assicurazione finché l'edificio non va in fiamme", ha affermato Rice. "Il modo migliore in cui un CSO può dimostrare la propria utilità agli altri dirigenti è spiegare… come i problemi di sicurezza possono mettere a rischio i profitti… specificando che un dollaro speso oggi può potenzialmente farne risparmiare milioni in futuro".

Molto dipende dal proprio status all'interno dell'azienda. "Se il CSO non riporta direttamente al CEO, probabilmente occupa una posizione troppo bassa nella scala gerarchica aziendale".

Oltre tre quarti dei dirigenti IT e della sicurezza intervistati, ovvero il 77%, hanno dichiarato che la propria azienda aveva un chief information security officer. Quasi la metà, il 46%, ha affermato che il CISO riportava direttamente al CEO.

L'introduzione di incentivi per il miglioramento della sicurezza è un'altra area in cui diversi esperti ritengono che il governo possa svolgere un ruolo importante. Anche se gli effetti delle normative (di cui parleremo in maniera più approfondita nel capitolo 4) sono complessi, alcuni hanno individuato altri modi in cui l'azione governativa può modificare gli incentivi per la sicurezza.

"La sfera informatica è uno sgabello a tre gambe", ha affermato il generale in pensione Michael Hayden, aggiungendo che queste tre gambe sono "la semplicità d'uso, la sicurezza e la privacy… Finora, quasi tutte le nostre energie creative sono state dedicate alla semplicità d'uso".

"Quando manca una delle tre gambe, lo sgabello traballa" ha commentato, aggiungendo che il paradigma secondo cui la semplicità d'uso è prioritaria rispetto alle altre due gambe deve assolutamente cambiare.

La fiducia nel proprio livello di preparazione è variabile

Quasi un terzo dei dirigenti IT intervistati ha affermato che il proprio settore era "totalmente impreparato" o "non molto preparato" ad affrontare attacchi o infiltrazioni da parte di avversari di alto livello. Fra coloro che hanno effettivamente subito attacchi di questo tipo, la mancanza di fiducia sale al 41%.

Ma sono state registrate variazioni significative tra una nazione e l'altra. In Arabia Saudita, addirittura il 90% degli intervistati ha affermato che il proprio settore era impreparato ("totalmente impreparato" o "non molto preparato"). Nella maggior parte dei paesi, coloro che hanno subito attacchi di alto livello hanno manifestato la tendenza a essere più pessimisti sul proprio livello di preparazione: il 68% delle vittime indiane e il 75% delle vittime messicane ha giudicato impreparato il proprio settore.

I paesi in cui i dirigenti sono risultati più fiduciosi circa il livello di preparazione per gli attacchi di alto livello sono stati la Germania (78%) e il Regno Unito (64%).

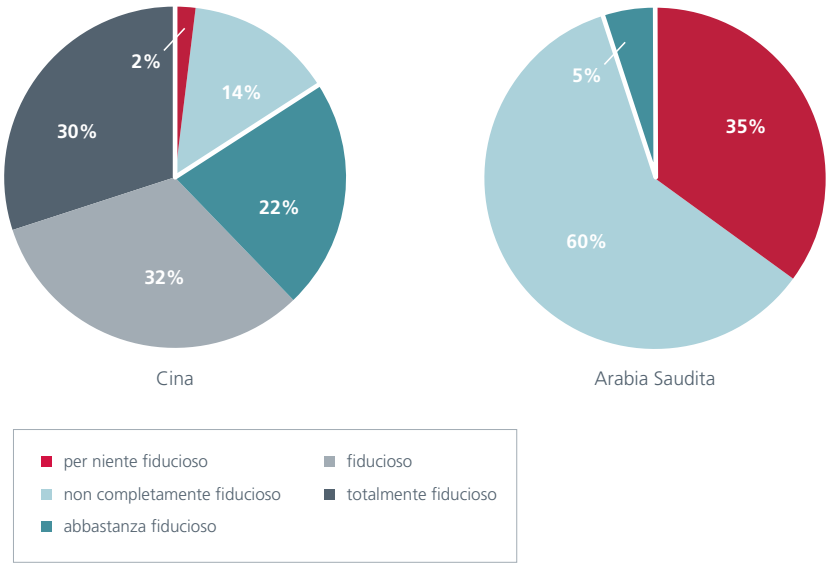
A parte gli attacchi DDoS di alto livello, in genere i dirigenti hanno giudicato il proprio settore più preparato nei confronti di altre forme di attacco; solo uno su quattro ha dichiarato che il proprio settore era impreparato a questo riguardo.

Rispetto allo spettro completo delle minacce attuali, i dirigenti di Stati Uniti, Regno Unito e Australia hanno costantemente attribuito ai propri settori il livello di preparazione più elevato. In tutti questi paesi sono stati avviati programmi di alto profilo per garantire il supporto del governo ai proprietari e ai gestori delle infrastrutture critiche.

Dubbi sulla capacità del sistema bancario e telefonico di resistere a un attacco

I dirigenti IT dubitavano inoltre che i propri fornitori di infrastrutture critiche fossero in grado di offrire un servizio affidabile in caso di attacco informatico di grandi proporzioni. Il 30% riteneva che il proprio fornitore di servizi bancari o altri servizi finanziari non lo fosse. E il 31% nutriva gli stessi dubbi sul proprio fornitore di telecomunicazioni. Il tasso di fiducia più basso nei confronti della capacità di resistenza del sistema bancario è stato registrato in alcuni paesi europei: Italia, Francia e Spagna.

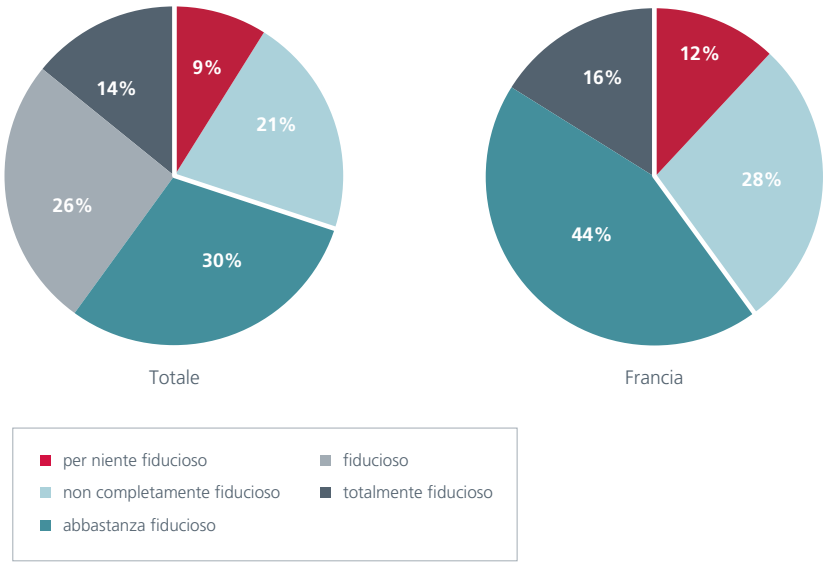
Fiducia nella capacità dei servizi governativi di resistere a un attacco informatico di grandi proporzioni



Durante gli attacchi DDoS lanciati contro l'Estonia nel 2007, i siti web di molte banche del paese sono stati messi fuori uso, anche se in seguito è stato dichiarato che i sistemi operativi non erano stati compromessi. Gli specialisti di sicurezza di vari settori e paesi concordavano sul fatto che i servizi bancari e finanziari tendono ad avere livelli di sicurezza più elevati. Ma allo stesso tempo risentono del "fattore Willy Sutton": quando gli fu chiesto perché rapinava le banche, il famoso bandito americano rispose enigmaticamente "perché è lì che stanno i soldi". In altre parole, i cybercriminali motivati da interessi economici saranno sempre attratti da questo settore.

Il livello di fiducia nei confronti dei servizi governativi è risultato più alto rispetto alla maggior parte degli altri settori. Nonostante questo, solo il 37% degli intervistati riteneva che il proprio governo fosse in grado di continuare a fornire i propri servizi in caso di attacco informatico di grandi proporzioni. I tassi di fiducia più bassi e più alti sono stati registrati rispettivamente in Arabia Saudita e in Cina.

Fiducia nella capacità dei servizi bancari e finanziari di resistere a un attacco informatico di grandi proporzioni



Contrastare la minaccia: misure di sicurezza

Alcune misure di base fondamentali non sono adottate su larga scala.

Ai dirigenti responsabili dell'IT e della sicurezza è stata posta una serie di domande dettagliate su oltre venti misure di sicurezza (tecnologie, policy e procedure) e sulle relative modalità di utilizzo.

Ai responsabili dei sistemi SCADA o ICS (Industrial Control System) della propria azienda è stata posta una serie analoga di domande sulle misure implementate in queste reti. I dati relativi a SCADA/ICS, benché basati su un campione più ridotto di intervistati, sono impressionanti. Più di tre quarti dei responsabili SCADA/ICS hanno dichiarato che i sistemi erano connessi a Internet o a un'altra rete IP. Fra questi, quasi la metà ha ammesso che la connessione creava un "problema di sicurezza irrisolto".

Le altre risposte, analizzate domanda per domanda, rivelano che alcune fondamentali misure di sicurezza di base non sono adottate su larga scala.

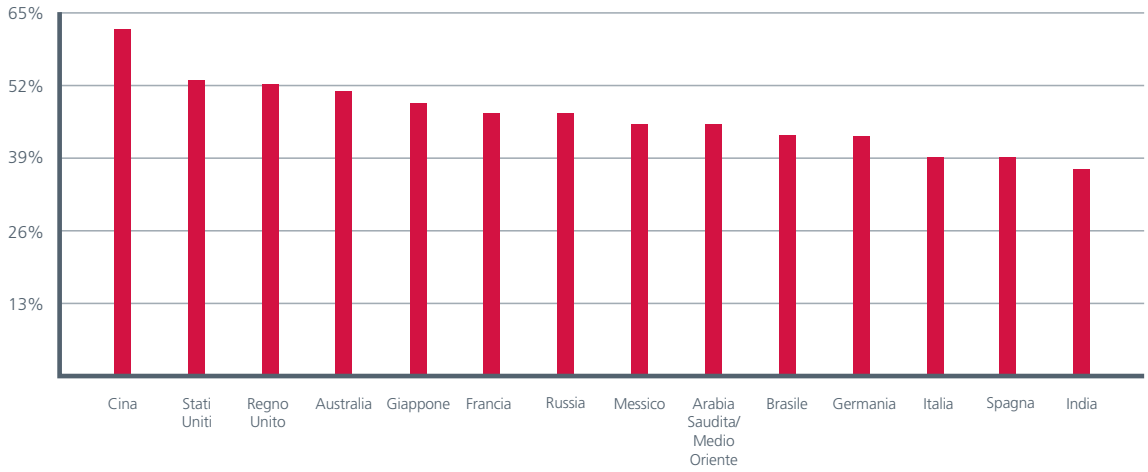
Il consolidamento di questi dati mostra i paesi e i settori che hanno i tassi di adozione generalmente più alti e più bassi in relazione a queste misure di sicurezza. Non si tratta necessariamente di un giudizio "positivo" o "negativo" sulla sicurezza di un settore o di un paese specifico, ma questi dati forniscono comunque un quadro delle procedure di sicurezza basato sul tasso di implementazione oggettivo delle misure di sicurezza chiave e non sull'autovalutazione soggettiva degli intervistati.

Utilizzando questo parametro, la Cina ha registrato il tasso di adozione più elevato (62%), distaccando notevolmente i paesi con i tassi di adozione immediatamente successivi (50-53%): Stati Uniti, Regno Unito e Australia.

Italia, Spagna e India hanno registrato i tassi di adozione più bassi, tutti al di sotto del 40%. Gli altri paesi, Giappone, Russia, Francia, Arabia Saudita, Messico, Brasile e Germania, si sono collocati tutti nella fascia compresa fra il 40 e il 49%.

I settori con i tassi di adozione più elevati sono risultati quello bancario e quello energetico. Il tasso più basso è stato registrato nel settore idrico/fognario.

Tassi di adozione delle misure di sicurezza riferiti dagli intervistati



Tasso di adozione delle misure di sicurezza (SMAR)

Ai dirigenti IT e della sicurezza sono state poste domande su 27 misure di sicurezza differenti: dieci tecnologie di sicurezza, sei policy di sicurezza, cinque modi diversi di usare la crittografia e sei modalità di autenticazione obbligatoria. Lo SMAR (Security Measure Adoption Rate) indica sostanzialmente il numero di risposte affermative alle domande sull'uso di una misura specifica.

Ogni azienda ha una strategia di sicurezza personalizzata, e molte delle misure su cui sono stati interpellati i dirigenti possono essere usate in vari modi. Il tasso SMAR, pertanto, non esprime necessariamente un giudizio "positivo" o "negativo" sulla sicurezza di un determinato settore o paese, ma consente di effettuare valutazioni comparative del tasso di adozione delle misure di sicurezza chiave nei vari settori e nelle varie nazioni. Si tratta di una misura approssimativa, perché a ogni tecnologia, procedura o policy viene attribuito lo stesso peso indipendentemente dalla sua efficacia, ma di fatto oggettiva.

I dirigenti cinesi hanno riferito il tasso adozione di gran lunga più elevato: 62%

I tassi di adozione riferiti sono stati superiori a quelli di qualunque altro paese per tutti i tipi di misure di sicurezza. Gli Stati Uniti, con un tasso di adozione del 53%, e l'Australia e il Regno Unito, rispettivamente con il 51 e il 52%, sono risultati i paesi con i tassi più alti dopo la Cina.

Italia, Spagna e India hanno registrato i tassi di adozione più bassi, tutti al di sotto del 40%. Gli altri paesi, Giappone, Russia, Francia, Arabia Saudita, Messico, Brasile e Germania, si sono collocati tutti nella fascia compresa fra il 40 e il 49%.

I tassi di adozione più elevati riducono la percentuale di successo degli attacchi?

Questa è una domanda cruciale, ma le risposte fornite dall'indagine non sono risolutive. La Cina, con il suo elevato tasso di adozione delle misure di sicurezza, ha in effetti un tasso di incidenza inferiore rispetto ai paesi che si collocano ai livelli più bassi della scala SMAR, ad esempio l'India. Anche altri dati indicano che le nazioni con i tassi di adozione più bassi corrono rischi maggiori. La divisione di intelligence globale delle minacce di McAfee, ad esempio, esegue un monitoraggio del traffico elettronico dannoso che proviene dai computer delle botnet dopo che sono stati infettati. I dati indicano che l'India, la nazione con il più basso tasso di adozione delle misure di sicurezza, è al primo posto nella classifica del traffico dannoso in Asia, con una quantità superiore a quella di Russia e Cina nel loro insieme.

D'altro canto, lo stato di sicurezza generale della Cina non è visibilmente migliore di quello di molti altri paesi con tassi di adozione decisamente inferiori. La Cina non è esente da attacchi di alto livello, né gli intervistati cinesi si considerano più preparati rispetto a quelli delle altre nazioni.

Alcune misure chiave non sono adottate su larga scala

La tecnologia di sicurezza meno adottata è risultata il whitelisting delle applicazioni, implementato solo da meno di un quinto delle aziende (19%) sia nelle reti SCADA/ICS che nelle reti IT. Altre tecnologie di sicurezza più avanzate, ad esempio i sistemi SIEM (Security Information and Event Management) e gli strumenti di rilevamento dei ruoli e delle anomalie, sono state impiegate rispettivamente dal 43% e dal 40% delle aziende.

Cina e India a confronto

Cosa spiega l'enorme differenza tra i tassi di adozione delle misure di sicurezza in queste due potenze asiatiche? Entrambe si considerano sottoposte a normative severe. In India, più dirigenti che in qualsiasi altro paese (il 97%) hanno indicato che la propria sicurezza informatica è regolamentata dal punto di vista normativo, mentre la Cina, con il 92%, si è collocata al secondo posto insieme alla Germania. Ma l'atteggiamento nei confronti delle disposizioni governative varia considerevolmente. In Cina il 91% dei dirigenti ha dichiarato di aver modificato le procedure aziendali in base alle normative, mentre la percentuale indiana è stata solo del 66%. L'India ha anche registrato livelli molto bassi di partecipazione alle partnership fra governo e infrastrutture critiche, mentre la Cina ha registrato il livello più elevato.

I dirigenti cinesi, inoltre, hanno espresso livelli di fiducia più alti nella capacità di deterrenza e prevenzione degli attacchi informatici da parte del governo. I dati del servizio di intelligence globale delle minacce di McAfee indicano che l'India ha recentemente sostituito la Cina (nonché la Russia e la Romania) come terreno di caccia privilegiato per gli hacker alla ricerca di computer infetti per le botnet, un'altra possibile conseguenza della disparità fra i due paesi a livello di adozione delle misure di sicurezza.

I dirigenti cinesi hanno riferito il tasso adozione di gran lunga più elevato.

Gli esperti hanno affermato che i vantaggi di alcuni strumenti di nuova generazione potrebbero non essere stati compresi dal mercato, oppure potrebbero essere adatti solo per le grandi aziende.

Ma anche alcune misure di sicurezza molto più elementari hanno una diffusione molto ridotta. Solo il 57% di tutti i dirigenti ha dichiarato che la propria azienda esegue regolarmente l'aggiornamento e l'applicazione delle patch per il software. L'applicazione periodica delle patch è risultata una procedura diffusa in Arabia Saudita (80%), Russia (77%) e Australia (73%) e meno comune in Brasile (37%).

Inoltre, solo un terzo dei dirigenti ha affermato che la propria azienda disponeva di policy "che limitano o proibiscono l'uso di chiavette USB o altri supporti rimovibili". Al di là del rischio che i dati vengano scaricati, sottratti e portati al di fuori dell'azienda, questi supporti, anche quando vengono utilizzati in buona fede, possono facilmente diffondere virus e altro malware, anche nei sistemi protetti da firewall. Il divieto di usare chiavette USB e altri supporti simili è risultato più diffuso in Arabia Saudita (65%) e in Russia (50%) e più raro in Spagna (13%) e in Brasile (20%).

Altre misure sono più diffuse

La misura di sicurezza più ampiamente adottata sono i firewall tra reti private e pubbliche, utilizzati dal 77% degli intervistati (65% per i sistemi SCADA e ICS).

I servizi di intelligence per il monitoraggio delle minacce sono più diffusi in India (57%), Cina (54%) e Giappone (54%) e meno comuni in Arabia Saudita (20%), Russia (23%) e Italia (20%).

Variazioni significative nell'uso della crittografia

Anche nel caso della crittografia la Cina ha registrato i tassi di adozione più elevati. L'unica eccezione riguardava l'uso della crittografia per proteggere i dati di CD e altri supporti rimovibili, un'area in cui la Cina, con il suo 48%, si è collocata alle spalle di Stati Uniti (56%), Giappone e Regno Unito (54%). L'India ha riportato tassi di adozione più bassi della media per cinque tipi di utilizzo della crittografia su sei. Anche Italia e Spagna hanno riferito tassi di adozione al di sotto della media per la crittografia.

Il settore idrico/fognario ha i tassi di adozione più bassi

I settori con i tassi di adozione più elevati sono risultati quello dei servizi bancari/finanziari e quello energetico, entrambi con il 50%. Il tasso più basso, 38%, è stato registrato nel settore idrico/fognario. Tutti gli altri settori si sono collocati nella fascia dal 40% in su.

Nel settore idrico/fognario sono stati registrati anche i più bassi tassi di adozione delle misure di sicurezza per la protezione dei sistemi SCADA/ICS. Uno dei motivi può essere che questo settore ha i livelli più bassi di connessione dei sistemi SCADA alle reti IP (solo 55% contro il 76% generale).

Quando si analizzano questi dati occorre ricordare che, fra i dirigenti responsabili di sistemi SCADA/ICS, quelli appartenenti al settore idrico erano solo 11 su 143.

L'80% ha riferito che i sistemi SCADA sono connessi a reti IP o a Internet, nonostante i rischi esistenti.

Sicurezza dei sistemi SCADA

Abbiamo creato una scala SMAR anche per i sistemi SCADA e ICS. Questa scala si basa sulle risposte fornite dai responsabili di questi sistemi in relazione a 16 misure di sicurezza e autenticazione. L'interpretazione di questi dati richiede una certa cautela per via del campione ridotto di intervistati: solo 143 dirigenti su 600 avevano responsabilità SCADA e hanno risposto a domande sui sistemi SCADA delle loro aziende.

Ancora una volta la Cina si è collocata al primo posto con un tasso di adozione delle misure di sicurezza SCADA/ICS pari al 74%, molto lontano dal 57% dell'Australia (secondo posto) e dal 54% del Brasile (terzo posto). Le variazioni dei tassi di adozione tra i vari paesi sono impressionanti. I più bassi tassi di adozione delle misure SCADA/ICS sono stati registrati in India e Spagna (29%) e nel Regno Unito (31%). Questi dati indicano che gli operatori SCADA/ICS cinesi hanno raggiunto un livello di adozione quasi triplo rispetto agli operatori indiani e spagnoli.

Nella fascia centrale si sono collocati Stati Uniti e Giappone (50%), seguiti da Francia, Russia, Germania e Arabia Saudita (dal 40% in su) e quindi da Italia e Messico (rispettivamente 38 e 35%).

Alcuni strumenti come il whitelisting delle applicazioni e i sistemi SIEM sono risultati più diffusi nei sistemi SCADA/ICS che nelle reti IT.

Molti dirigenti hanno riferito elevati livelli di connessione dei sistemi SCADA alle reti IP o a Internet nonostante la consapevolezza diffusa dei rischi.

Il 76% degli intervistati con responsabilità SCADA/ICS ha dichiarato che le proprie reti erano "connesse a una rete IP o a Internet". Fra questi, quasi la metà (47%) ha ammesso che la connessione creava un "problema di sicurezza irrisolto".

Le connessioni alle reti IP rappresentano una vulnerabilità perché potrebbero consentire a utenti non autorizzati di accedere ai sistemi strategici dell'infrastruttura critica, ha commentato un dirigente della sicurezza IT con una lunga esperienza alle spalle. "La concezione SCADA originale non prevedeva che i sistemi di controllo sarebbero stati collegati a reti in cui persone non autorizzate possono accedere a vari livelli a questi sistemi". Il software SCADA è stato in larga parte scritto "molto tempo fa e non è stato modificato da allora". I sistemi "non vengono eseguiti sulle piattaforme più recenti e risentono quindi delle vulnerabilità che sono state scoperte nel corso del tempo".

Poiché spesso i sistemi SCADA comprendono sia hardware che software, non è possibile aggiornarli come il software normale e la loro sostituzione è un'operazione "estremamente complessa e costosa", ha aggiunto il dirigente. Non esiste "alcun meccanismo per riconsiderare e modificare i sistemi quando vengono individuate delle vulnerabilità".

Uno specialista di sicurezza informatica del settore energetico ha affermato che i sistemi SCADA sono stati "concepiti come ambienti destinati a un'utenza tecnica" con funzioni di sicurezza ridotte. In genere si tratta di sistemi "aperti e difficili da proteggere".

Secondo alcuni esperti, le reti SCADA/ICS non dovrebbero essere connesse a Internet. Punto. "I sistemi di controllo dovrebbero avere un'infrastruttura dedicata e non essere connessi alla rete Internet generale" ha affermato uno specialista del settore dei trasporti, aggiungendo che in alcuni casi, a suo parere, le reti ICS vengono connesse a Internet "per pura comodità".

Il worm Conficker, diffuso tramite Internet, ha rappresentato una sorta di campanello d'allarme, ha aggiunto lo specialista del settore energetico. Il worm "ha raggiunto sistemi che in teoria avrebbero dovuto essere inaccessibili, suscitando notevoli preoccupazioni".

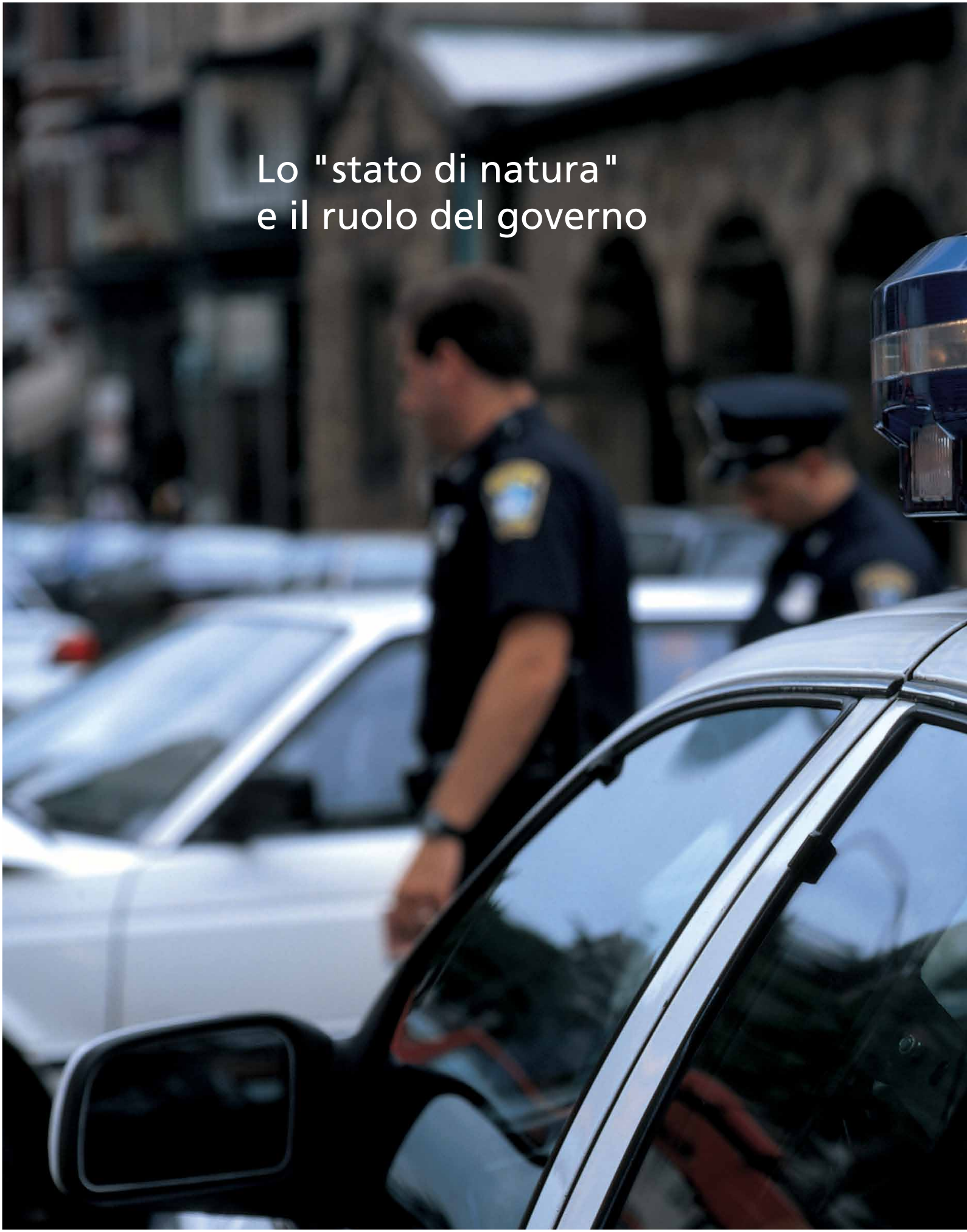
Ma gli esperti hanno anche dichiarato che la consapevolezza delle vulnerabilità dei sistemi SCADA stava aumentando, una realtà confermata dai dati dell'indagine.

"Solo cinque anni fa", ha commentato lo specialista del settore dei trasporti, "se andavi nelle grandi aziende di questo o altri settori e parlavi con i responsabili della sicurezza informatica… ti rendevi conto che non avevano alcuna conoscenza dei sistemi di controllo; in molto casi non sapevano neppure che esistessero, cosa fossero e come funzionassero perché questi sistemi non rientravano nella sfera di competenza dei CIO e dello staff di sicurezza informatica dell'azienda. Erano di competenza dello staff operativo e alla sicurezza informatica non veniva prestato alcun tipo di attenzione".

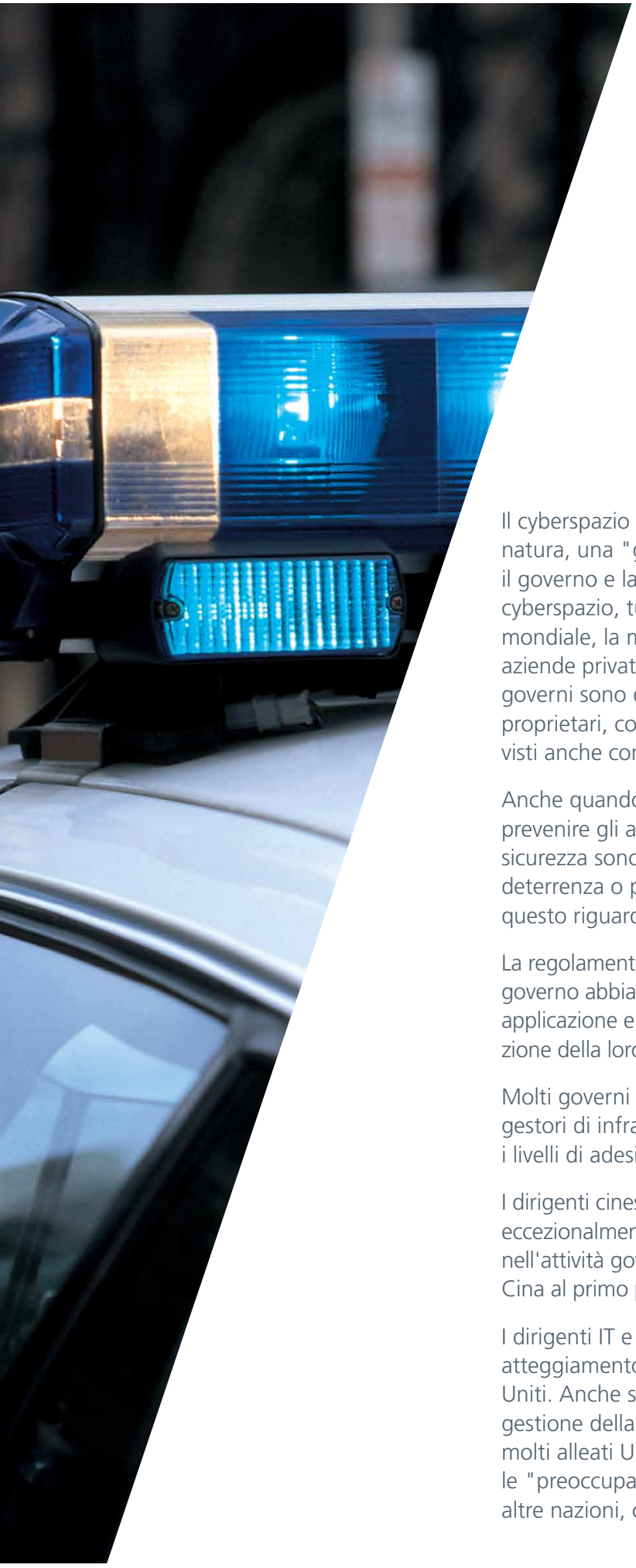
"Credo che si possa tranquillamente affermare" ha concluso lo specialista "che stanno cercando tutti di recuperare il tempo perso".

Il 92% dei dirigenti con responsabilità SCADA ha dichiarato di adottare qualche forma di monitoraggio dei sistemi. Gli strumenti di analisi del comportamento di rete sono risultati le misure più diffuse (62% totale), con Cina (100%), Regno Unito (78%) e Messico (75%) in testa alla classifica dei tassi di adozione. Il 59% degli intervistati utilizzava i registri di verifica, con Germania (90%) e Cina (82%) ai primi posti.

Solo l'8% ha affermato di non eseguire il monitoraggio delle nuove connessioni IP ai sistemi SCADA/ICS.



Lo "stato di natura" e il ruolo del governo



I dirigenti IT ritengono che gli Stati Uniti siano il paese che suscita le "preoccupazioni maggiori" a livello di attacchi informatici contro altre nazioni.

Il cyberspazio somiglia molto a quello che Hobbes definiva stato di natura, una "guerra di tutti contro tutti". Hobbes riteneva che solo il governo e la legge potessero mettere fine a questa guerra. Nel cyberspazio, tuttavia, il ruolo del governo è più complesso. A livello mondiale, la maggior parte delle infrastrutture critiche è nelle mani di aziende private che spesso operano in più paesi. Per queste aziende i governi sono di volta in volta partner, organi di controllo e vigilanza, proprietari, contractor e clienti. Allo stesso tempo, tuttavia, vengono visti anche come aggressori, infiltrati e avversari.

Anche quando i governi svolgono un ruolo di difesa, cercando di prevenire gli attacchi e migliorare la sicurezza, molti dirigenti IT e della sicurezza sono scettici sulla loro capacità di svolgere una funzione di deterrenza o protezione dagli attacchi informatici. L'atteggiamento a questo riguardo, tuttavia, varia sensibilmente da un paese all'altro.

La regolamentazione normativa è una delle aree in cui si ritiene che il governo abbia un impatto generalmente positivo. I tassi di verifica e applicazione e l'impatto delle normative di sicurezza, nonché la percezione della loro efficacia, variano considerevolmente da un paese all'altro.

Molti governi hanno promosso la collaborazione tra proprietari e gestori di infrastrutture critiche in materia di sicurezza informatica, ma i livelli di adesione sono risultati estremamente variabili.

I dirigenti cinesi riferiscono un livello di collaborazione con il governo eccezionalmente elevato, nonché alti livelli di regolamentazione e fiducia nell'attività governativa. Questi dati collocano sorprendentemente la Cina al primo posto per quanto riguarda l'intervento governativo.

I dirigenti IT e della sicurezza di tutto il mondo manifestano un atteggiamento estremamente ambivalente nei confronti degli Stati Uniti. Anche se sono la nazione citata più spesso come modello per la gestione della sicurezza informatica, i dirigenti di molti paesi, compresi molti alleati USA, ritengono che gli Stati Uniti siano il paese che suscita le "preoccupazioni maggiori" a livello di attacchi informatici contro le altre nazioni, con la Cina poco distanziata al secondo posto.

Percentuale secondo cui l'attuale legislazione nazionale è inadeguata per la lotta agli attacchi informatici

Dubbi sulla capacità di governi e leggi di svolgere una funzione di deterrenza nei confronti degli aggressori

Più della metà dei dirigenti intervistati riteneva che le leggi del proprio paese fossero inadeguate a livello di deterrenza degli attacchi informatici. Questa opinione è stata espressa da più di tre quarti dei dirigenti russi e da una cospicua maggioranza di quelli messicani e brasiliani. Il livello di fiducia più elevato nei confronti della capacità di deterrenza delle leggi nazionali è stato registrato in Germania, seguita da Francia e Stati Uniti.

In alcuni paesi sono stati inoltre espressi dubbi sulla capacità del governo di prevenire e scoraggiare gli attacchi. Un sorprendente 45% riteneva che il proprio governo avesse capacità di prevenzione e deterrenza "scarse" o "nulle" nei confronti degli attacchi informatici. In paesi come Brasile e Italia, almeno due terzi degli intervistati giudicavano "scarse" o "nulle" le capacità del governo a questo riguardo. Anche in Messico, Arabia Saudita, Germania e Spagna la maggioranza degli interpellati ha espresso opinioni negative sulle capacità del governo. Negli Stati Uniti, al contrario, solo il 27% dei dirigenti riteneva che il governo avesse capacità scarse o nulle. Il voto di "sfiducia" cinese è stato quasi altrettanto basso (30%).

"Lo sceriffo latita", ha affermato il generale in pensione Michael Hayden, che ha recentemente concluso una lunga carriera come funzionario senior dell'intelligence statunitense e direttore della CIA. A suo avviso, il cyberspazio può essere paragonato al leggendario Far West. "Poiché tutti devono difendersi, tutti girano armati". Ma applicare questo principio al cyberspazio equivarrebbe a pretendere che ogni cittadino organizzasse la propria difesa nazionale. "Nessuno andrebbe in un ufficio postale a chiedere come pensano di difendersi dai missili balistici… ma questo scenario sarebbe perfettamente in linea con l'attuale configurazione della sicurezza informatica", ha commentato Hayden.

Molti ritengono che le normative statali consentano di migliorare la sicurezza

Molti esperti concordavano sul fatto che i governi devono fare di più per migliorare la sicurezza informatica delle infrastrutture critiche, ma il panorama generale è estremamente variegato e presenta differenze significative a livello di approcci adottati, impatto delle normative e consenso da parte dei dirigenti IT nei vari paesi.

Nel complesso, l'86% dei dirigenti ha affermato che la sicurezza informatica del proprio paese era in qualche modo soggetta a leggi o normative statali. Quasi tre quarti (74%) hanno dichiarato che la propria azienda aveva "implementato nuove policy, procedure, best practice o misure tecniche"

Una cospicua maggioranza dei dirigenti IT ritiene che le normative e/o la legislazione hanno migliorato la sicurezza informatica.

per conformarsi a leggi o normative. Sono state registrate variazioni significative a livello nazionale, con i due estremi della scala rappresentati rispettivamente dalla Cina, dove il 91% ha modificato le policy in base alle regole governative, e dalla Spagna, con il 56%. Nella fascia centrale si sono collocate India, Germania, Italia e Australia, tutti paesi in cui meno del 70% degli intervistati ha modificato le proprie procedure.

Il 42% ha affermato che le normative statali "non producevano effetti significativi" o addirittura "sottraevano risorse al miglioramento della sicurezza"; il 58%, al contrario, riteneva che avessero consentito di "ottimizzare le policy e migliorare la sicurezza". In tutti i paesi in cui sono state registrate differenze di approccio significative a livello nazionale (Brasile, Spagna, Cina, Messico, Germania e Giappone), una percentuale compresa fra il 60 e il 70% concordava sul fatto che le normative avessero migliorato la sicurezza. I dubbi maggiori sono stati espressi in Italia e Australia, dove la maggior parte degli intervistati ha messo in discussione la validità del regime normativo del proprio governo.

La fiducia nell'efficacia delle normative è risultata particolarmente bassa nel settore idrico, dove solo il 24% riteneva che gli interventi normativi avessero migliorato la sicurezza. Anche in questo caso è opportuno sottolineare che in questo settore è stato interpellato un numero ridotto di persone.

Partecipazione e partnership

La collaborazione promossa dal governo per la sicurezza informatica varia enormemente fra i proprietari e i gestori di infrastrutture critiche.

La partecipazione alle partnership guidate dal governo è generalmente bassa. Per quanto riguarda il coinvolgimento nell'elaborazione di leggi e normative, circa un terzo dei dirigenti (35%) ha affermato che la propria azienda aveva preso parte a una partnership tra governo e settore privato. La partecipazione è risultata più alta a livello di iniziative orizzontali, ad esempio le associazioni di settore per la condivisione delle informazioni, a cui ha dichiarato di aver aderito più della metà degli intervistati (53%).

Ma il livello di partecipazione è risultato estremamente variabile nei vari paesi. La percentuale più alta è stata registrata in Cina, dove il 61% dei dirigenti ha dichiarato di aver aderito a una partnership con il governo. I tassi di partecipazione sono risultati estremamente ridotti in Brasile (22%) e inferiori al 30% anche in Giappone, Germania, Italia, India e Spagna.

I livelli di partecipazione, tuttavia, non forniscono necessariamente un'indicazione dell'effettivo successo di queste iniziative. Perfino negli Stati Uniti, dove la partecipazione alle partnership è relativamente elevata (42%), i dati delle interviste indicano chiaramente che il settore continua a considerare la condivisione delle informazioni un processo a senso unico.

La Cina è al primo posto a livello di intervento governativo

Nel complesso, quasi la metà dei dirigenti (49%) ha riferito che la propria azienda era stata sottoposta a verifiche di conformità con le leggi o le normative sulla sicurezza informatica da parte di un ente governativo. I tassi di verifica nei vari paesi, tuttavia, sono risultati estremamente variabili, con punte massime in Cina (83%) e Arabia Saudita (73%). Brasile, Australia e Francia hanno riferito livelli di verifica superiori al 50%. I tassi più bassi sono stati registrati in Russia (30%) e in Spagna (32%).

I dirigenti cinesi hanno riferito anche un elevato livello di attività normativa e legislativa da parte del governo; il 92% ha infatti dichiarato di essere soggetto a regolamentazioni di questo tipo. In questo ambito la Cina si è collocata al secondo posto insieme alla Germania, mentre l'India detiene il primato assoluto con il 97%.

Il paese in cui i dirigenti hanno riferito i più bassi livelli di attività normativa sono stati gli Stati Uniti, dove solo il 72% dei dirigenti, contro l'86% generale, ha dichiarato di essere soggetto a forme di regolamentazione della sicurezza informatica.

Gli Stati Uniti sono visti come modello

Questo potrebbe essere il motivo per cui la percentuale più elevata di dirigenti IT e della sicurezza (44%) ha indicato gli Stati Uniti come paese, escluso il proprio, da prendere a modello per la sicurezza informatica. Alle spalle degli Stati Uniti si sono collocati Germania (22%) e Regno Unito (18%). Il modello statunitense è risultato particolarmente apprezzato in Cina (78%) e in Messico (72%). La percentuale di consenso più bassa è stata registrata in Germania (31%).

I dati delle interviste lasciano intendere che il gradimento espresso nei confronti del modello statunitense potrebbe derivare dall'attenzione che stampa e funzionari di alto livello hanno dedicato agli sforzi degli Stati Uniti in questo ambito, più che dalle modalità con cui il governo USA gestisce il problema. Poche nazioni sembrano infatti emulare gli Stati Uniti a questo riguardo.

Origine dei dubbi sull'efficacia delle normative

Fra i dirigenti sono emerse preoccupazioni diffuse sull'impatto di leggi e normative. Questo dato, tuttavia, non è del tutto sorprendente; utilizzare le risposte dell'indagine per determinare gli atteggiamenti nei confronti delle normative può essere problematico. Pochi dirigenti chiedono di aumentare il livello di regolamentazione. Ma sono emersi alcuni punti chiave.

Gli intervistati hanno indicato tre aree di incertezza principali:

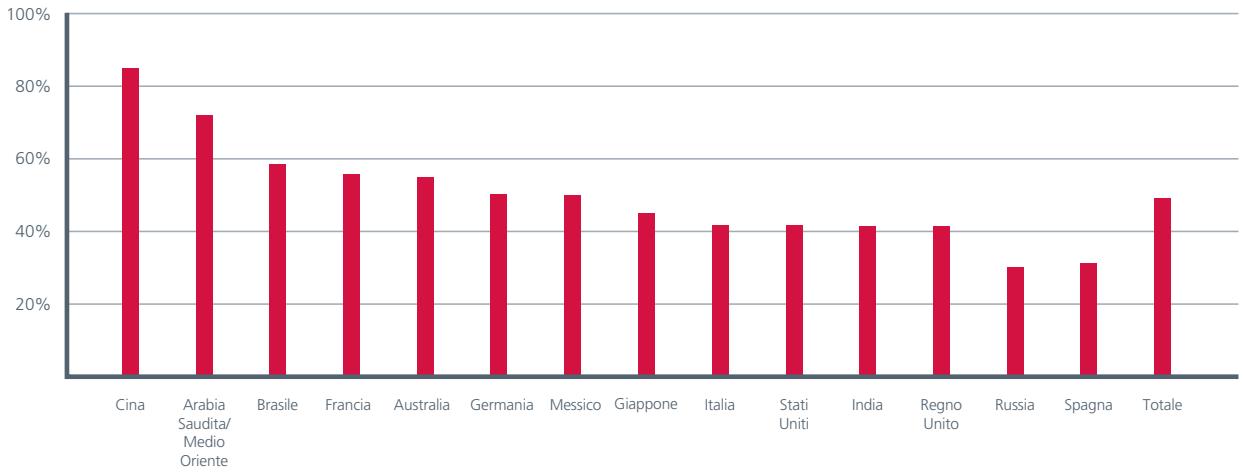
- Mancanza di fiducia nella capacità dei funzionari di comprendere le dinamiche del settore;
- Timore che normative inadeguate possano addirittura ridurre il livello di sicurezza in settori molto diversificati;
- Rischio che l'obbligo di denunciare gli incidenti di sicurezza (ad esempio la compromissione di dati personali) spinga policy e risorse in direzioni controproducenti.

I dubbi erano particolarmente diffusi nel settore idrico/fognario, in cui addirittura il 77% degli intervistati ha affermato che leggi e normative avevano "sottratto risorse al miglioramento della sicurezza" o non avevano prodotto alcun effetto. I dirigenti di questo settore hanno inoltre espresso il livello di fiducia più basso nella capacità del governo di svolgere una funzione di deterrenza o protezione dagli attacchi informatici.

Uno specialista di sicurezza statunitense del settore idrico/fognario ha affermato che gli obblighi normativi erano molto sentiti, soprattutto nelle aziende più piccole di un settore molto diversificato. "I membri del nostro staff sono costretti ad 'alimentare il mostro'... passano più tempo a rincorrere i requisiti normativi più disparati anziché a pianificare la sicurezza in maniera organica. "Cercare di soddisfare più 'padroni' è un'impresa folle che assorbe risorse preziose e in ultima analisi lascia al direttore dell'impianto la responsabilità (di decidere) come gestire il rischio".

Lo stesso specialista ha dichiarato che lui e i suoi colleghi "spesso si sentono come figli di un Dio minore" quando intervengono ai forum di sicurezza nazionali a cui partecipano tutti i settori. "In molti casi non riceviamo lo stesso tipo di considerazione che viene riservata agli altri settori, non a livello personale ma tattico e strategico", ha spiegato.

Percentuale che è stata oggetto di verifiche di conformità con leggi e/o normative da parte di un ente governativo



Ma i dubbi sull'efficacia delle normative non riguardano solo il settore idrico/fognario. I dati delle interviste indicano infatti che i dubbi nascono da preoccupazioni più diffuse.

"Qui negli Stati Uniti esiste una diffusa mancanza di fiducia nella capacità del governo di prendere provvedimenti adeguati e una mancanza di conoscenza (da parte del governo) del funzionamento delle varie infrastrutture", ha affermato uno specialista di sicurezza del settore dei trasporti. "Molti temono che le normative impongano una gran quantità di attività inutili e costose che hanno un effetto scarso o nullo sul miglioramento della sicurezza".

Gli esperti temono inoltre che nei settori molto diversificati le normative, soprattutto se applicate in maniera miope, potrebbero involontariamente "appiattire" gli standard di sicurezza. Definire un unico standard per un settore diversificato può migliorare la sicurezza di alcune entità; allo stesso tempo, tuttavia, disincentiva le aziende più sofisticate a superare la soglia stabilita. "Ho sentito di aziende che hanno abbassato i propri standard di gestione della sicurezza per conformarsi alla lettera alle normative", ha affermato uno specialista di sicurezza del settore energetico.

Molti temono che molte normative impongano "una gran quantità di attività inutili e costose che hanno un effetto scarso o nullo sul miglioramento della sicurezza".

I dirigenti hanno dichiarato che, a parte i guasti operativi, la conseguenza più temuta in caso di attacco informatico è il danno per la reputazione. Gli episodi riferiti indicano che, per via delle leggi che impongono di denunciare alle autorità determinati incidenti di sicurezza, le aziende potrebbero essere spinte a prendere decisioni che mirano a ridurre il numero di incidenti di questo tipo anziché a rafforzare la sicurezza generale dell'azienda.

In Giappone, ad esempio, un funzionario ha osservato che l'obbligo di denunciare alle autorità gli incidenti di sicurezza informatica ha suscitato una serie di lamentele. In alcuni casi, infatti, "gli obblighi amministrativi per il responsabile della sicurezza sono di gran lunga superiori alla (gravità della) minaccia".

Ma gli Stati Uniti sono considerati anche uno dei paesi più vulnerabili agli attacchi informatici

Il 50% dei dirigenti IT e della sicurezza ha anche indicato gli Stati Uniti come uno dei tre paesi "più vulnerabili agli attacchi informatici alle infrastrutture critiche del settore". Gli Stati Uniti guidavano la classifica, seguiti da Cina (34%) e Russia (27%).

La percezione della vulnerabilità statunitense è risultata particolarmente diffusa in Cina (dove l'80% ha indicato gli Stati Uniti come una delle tre nazioni più vulnerabili), Messico (73%), Brasile e Russia (70%).

La Cina è stata giudicata vulnerabile soprattutto dai dirigenti dei paesi vicini. I dirigenti di India (57%), Giappone (56%) e Australia (43%) l'hanno infatti inclusa fra le tre nazioni più vulnerabili con una frequenza superiore alla media.

Secondo alcuni esperti, gli Stati Uniti sono stati ritenuti più vulnerabili perché si tratta di un paese più avanzato, nonché di una delle nazioni con la più alta dipendenza dalle reti informatiche. Ma altri hanno fatto notare che la vulnerabilità degli Stati Uniti non ha nulla di eccezionale e può essere facilmente sopravvalutata.

Stati Uniti e Cina sono visti come probabili aggressori negli episodi di guerra informatica

Come osservato nel capitolo 1, una cospicua maggioranza di dirigenti IT e della sicurezza ritiene che i governi stranieri siano già stati coinvolti negli attacchi alle reti del proprio settore. Quando è stato chiesto di indicare il paese "che suscita le preoccupazioni maggiori a livello di attacchi alle reti del proprio paese/settore", il 36% ha citato gli Stati Uniti e il 33% la Cina (per questa domanda è stato proposto un elenco di sei paesi tra cui scegliere, ma gli intervistati avevano la possibilità di indicare anche una risposta diversa). Al terzo posto, con un notevole distacco, si è collocata la Russia (solo il 12%). Nessuno degli altri tre paesi (Regno Unito, Francia e Germania) ha superato il 6%.

Ogni settore nutriva preoccupazioni nei confronti di paesi diversi come potenziali aggressori. Fra i dirigenti del settore governativo, ad esempio, la Cina superava gli Stati Uniti come principale fonte di preoccupazione. I dirigenti delle aziende energetiche temevano soprattutto la Russia, quelli del settore delle telecomunicazioni si sentivano minacciati da Cina e Stati Uniti in egual misura.

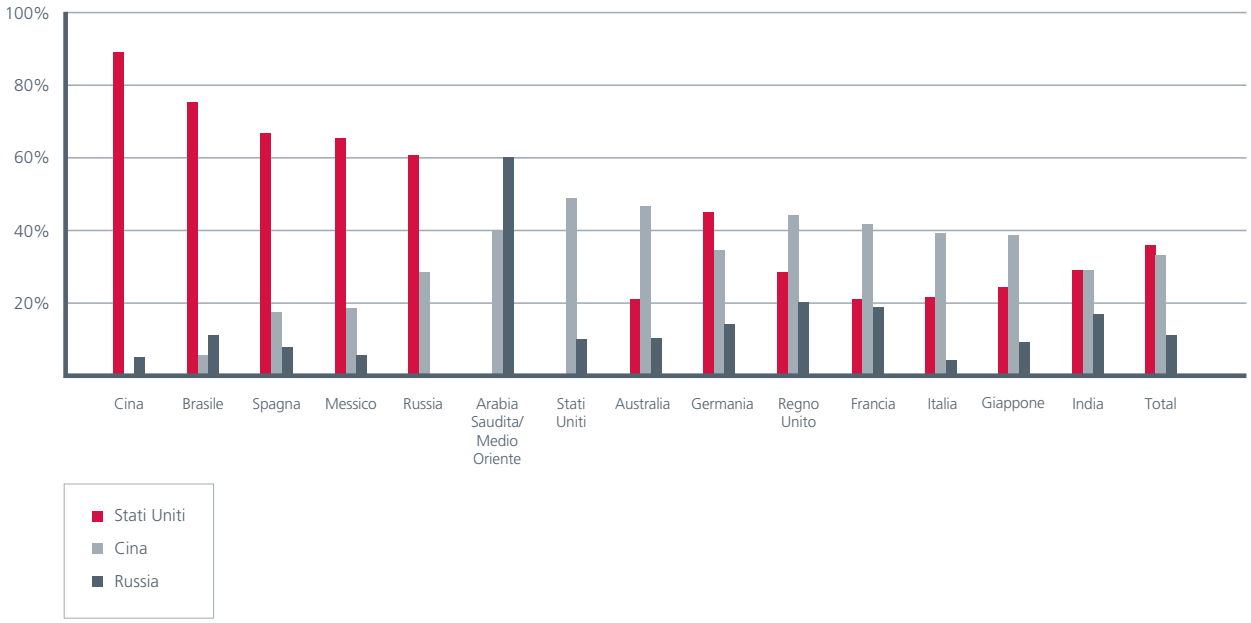
"Gli attacchi a cui dobbiamo far fronte [in Australia] sono di natura economica... dipende molto dal settore", ha affermato il dirigente australiano Ghosh. "Per il settore minerario la minaccia principale è rappresentata dalla Cina... In quello della difesa, i rivali sono Europa e Stati Uniti".

Gli Stati Uniti erano visti come il più temibile aggressore potenziale dalla maggior parte dei dirigenti i cui paesi sono tradizionalmente più sospettosi nei confronti degli USA: Cina (89%), Brasile (76%), Spagna (67%), Messico (65%) e Russia (61%). Ma anche in un alleato storico come la Germania il 45% ha indicato gli Stati Uniti come principale fonte di preoccupazione. Solo il 34% ha menzionato la Cina, anche se il governo tedesco ha pubblicamente rimproverato alla Cina di condurre attività di intelligence sulle reti informatiche delle sue risorse nazionali strategiche.

"Questo [risultato] potrebbe essere meno scioccante di quello che sembra", ha osservato Hayden. "Potrebbe essere influenzato dalla percezione delle capacità, o anche solo delle dimensioni, delle agenzie di intelligence statunitensi". Il governo statunitense ha anche avviato una serie di dibattiti pubblici, prolungati e in larga misura irrisolti su come organizzare la difesa delle proprie reti e le proprie capacità di attacco. Questa continua discussione pubblica potrebbe aver amplificato le preoccupazioni sulle capacità statunitensi, ha commentato Hayden.

Il dibattito statunitense ha sicuramente ricevuto un'attenzione maggiore da parte dei media, ma quest'anno anche i funzionari russi hanno messo in cantiere una serie di misure legislative per garantire alle autorità una maggiore libertà di azione nei confronti delle minacce e degli attacchi individuati. Una proposta di legge presentata di recente autorizzerebbe Mosca a definire gli atti di guerra informatica e prendere le contromisure necessarie. La nuova legge "prevede essenzialmente che, una volta appurato di aver subito un attacco informatico di qualsiasi tipo da parte del governo di un altro stato, le autorità russe possono considerarlo un atto di guerra," ha affermato Kimberly Zenz, esperta di questioni russe di iDefense Labs.

Percentuale che ha indicato USA, Cina o Russia come paese che suscita le "preoccupazioni maggiori" a livello di attacchi informatici contro le altre nazioni



Nel loro insieme, i nuovi provvedimenti legislativi conferiscono di fatto maggiori poteri al Cremlino, ha affermato. "In caso di incidente di grandi proporzioni, possono decidere autonomamente di cosa si trattava e prendere iniziative di livello molto alto senza aspettare consensi o prove dall'esterno".

Anche la Cina ha diffuso informazioni sui suoi piani di guerra informatica. Un rapporto sulla letteratura militare cinese pubblicato nel 2009 dalla USCC (U.S.-China Economic and Security Review Commission) ha concluso che "la dottrina cinese ha individuato nell'instaurazione precoce della predominanza informatica sul nemico una delle principali priorità operative di un conflitto". Nel rapporto si osservava inoltre che la nuova strategia denominata "Integrated Network Electronic Warfare", che prevede l'integrazione delle tecniche di guerra informatica o comunque elettronica con le operazioni di guerra tradizionali, sembrava essere stata concepita proprio per raggiungere questo obiettivo.

Nonostante queste discussioni, esistono limiti evidenti alla trasparenza. Sia Russia che Cina, ad esempio, hanno ricevuto (e categoricamente smentito) accuse ben documentate di collusione con gli hacker nazionalisti. Questi tre paesi vogliono palesemente continuare ad avvalersi, in misura maggiore o minore, del vantaggio strategico offerto dalla "negazione plausibile" nel cyberspazio.

Come possiamo uscire dallo "stato di natura"?

Finché i governi dei maggiori paesi continueranno a reclamare una libertà operativa incondizionata nel cyberspazio, non sarà possibile uscire da questa situazione di Far West. Nel frattempo, i proprietari e i gestori delle infrastrutture critiche che costituiscono questo nuovo campo di battaglia continueranno a rimanere nel mirino, e probabilmente dovranno provvedere autonomamente alla propria difesa.

Migliorare la sicurezza in un'era di guerra informatica

Quando si tratta di individuare strategie per il miglioramento della sicurezza informatica, i dati non offrono risposte esaurienti.

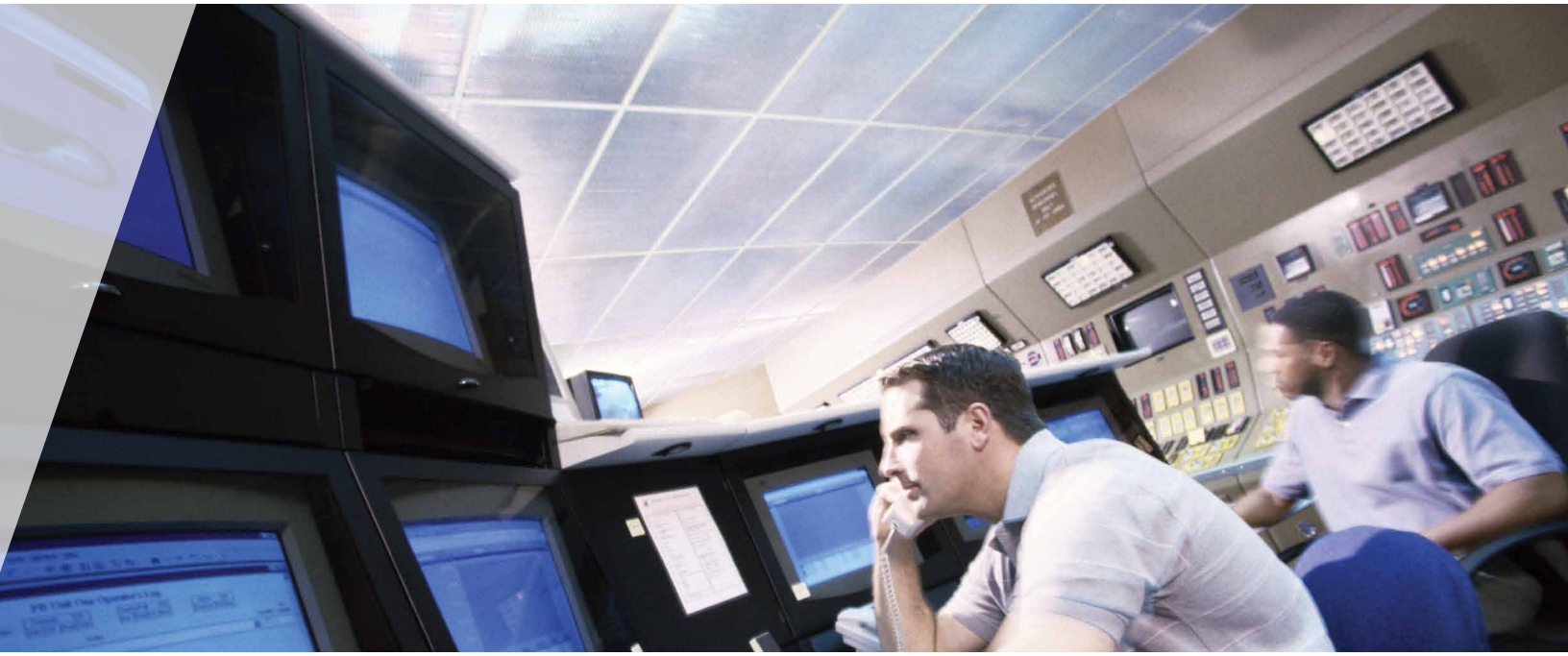
Quando si tratta di individuare strategie finalizzate a ottimizzare la sicurezza informatica delle infrastrutture critiche, i dati del sondaggio non sono in grado di offrire risposte esaurienti.

Proprietari e operatori di infrastrutture critiche dichiarano che la sicurezza è per loro di vitale importanza e ciò è facilmente riscontrabile nella grande quantità di misure di protezione implementate. Tuttavia, anche i settori e i paesi dove il tasso di implementazione di misure di sicurezza efficaci è più elevato non sono immuni da attacchi.

"Non esiste un modello di protezione preciso in grado di stare al passo con l'evoluzione e il livello di sofisticazione delle minacce informatiche", afferma Michael Assante, dal settore energetico. Inoltre, le tecnologie innovative, dal cloud computing alle "reti intelligenti" di gas ed elettricità, fino alla connettività SCADA, continuano a creare nuove vulnerabilità.

Anche i governi sono alla ricerca della migliore strategia di sicurezza informatica per la loro infrastruttura. Due sono le sfide che accomunano i loro sforzi:

- Modificare le vecchie strutture e organizzazioni governative in modo da poter affrontare le minacce informatiche che colpiscono le infrastrutture critiche.
- Trovare modi utili per condividere le informazioni sensibili su minacce e vulnerabilità con proprietari e operatori e per implementare capacità adeguate in grado di aiutare le infrastrutture critiche a difendersi.



Alcune tecnologie di sicurezza fondamentali non sono sufficientemente sfruttate.

Gli standard di autenticazione, in particolare, devono essere migliorati e l'impiego della tecnologia biometrica resta poco diffuso. La sicurezza della rete dipende sempre di più dal rilevamento e blocco di utenti i cui account evidenziano un comportamento anomalo o non sono conformi a una serie di privilegi rigorosamente definita. Inoltre, gli hacker si accaniscono sempre di più sui singoli utenti mediante attacchi di phishing e altre simili strategie. Questi sviluppi indicano chiaramente che l'autenticazione degli utenti e dei relativi privilegi è di importanza sempre più cruciale.

Tuttavia, più della metà (57%) dei dirigenti intervistati ha dichiarato che nelle rispettive aziende vengono utilizzati solo nomi utente e password per autenticare gli accessi, mentre il restante 43% ha affermato di utilizzare tecniche di autenticazione più rigorose, quali dati biometrici o token, sia singolarmente che in combinazione tra loro. In generale, solo il 16% ha dichiarato di avere implementato dispositivi biometrici, un tasso di adozione piuttosto basso che alcuni esperti attribuiscono, in molti paesi, a resistenze di tipo culturale. I token hanno una diffusione doppia. L'uso di token e sistemi biometrici comporta tuttavia anche svantaggi, problematiche tecniche e costi elevati, secondo quanto affermano gli esperti del settore, e le combinazioni password/ID di accesso possono variare sensibilmente in efficacia, a seconda della forza delle password impiegate e della tecnologia di crittografia utilizzata. Tuttavia, livelli aggiuntivi di sicurezza sono chiaramente preferibili rispetto al semplice impiego di nomi utente e password, spesso troppo facili da indovinare, trafugare o compromettere in qualsiasi altro modo.

Analogamente, a livello globale, solo la metà circa dei dirigenti ha dichiarato di utilizzare strumenti di crittografia nella maggior parte delle attività di routine, anche se la trasmissione dei dati online risulta l'ambito di maggiore impiego di questa tecnologia, con il 61% degli intervistati che afferma di servirsene. Si tratta comunque di una percentuale piuttosto bassa, vista la grande diffusione di dispositivi portatili. Pamela Warren, specialista McAfee in sicurezza informatica, ritiene che "se si utilizzano dispositivi portatili in cui sono archiviati dati sensibili, è assolutamente necessario implementare strumenti di crittografia".

Le vulnerabilità sono in continua espansione

L'uso sempre più diffuso di reti IP per sistemi SCADA e altri sistemi di controllo operativo crea vulnerabilità eccezionali e preoccupanti. I dirigenti che si occupano della gestione di sistemi SCADA/ICS hanno segnalato elevati livelli di connessione di tali sistemi con reti IP, inclusa Internet, pur riconoscendo che tali connessioni sono fonte di gravi preoccupazioni relative alla sicurezza. Gli esperti del settore si sono dichiarati seriamente allarmati dalle implicazioni di sicurezza di questi sviluppi e gli specialisti in sicurezza IT hanno sottolineato la necessità di contenere questa minaccia.

L'accesso remoto a sistemi di controllo "rappresenta un enorme pericolo", ha dichiarato Phyllis Schneck, vicepresidente McAfee per l'intelligence sulle minacce. "È necessario implementare misure di protezione appropriate oppure passare a reti private, senza utilizzare Internet", ha aggiunto Schneck, membro della commissione per la sicurezza informatica del CSIS per la presidenza Obama.

Oltre la metà degli intervistati ha dichiarato che nelle rispettive aziende vengono utilizzati solo nomi utente e password per autenticare gli accessi.

"Esiste un livello di protezione facilmente ottenibile mediante la virtualizzazione del software più vecchio in aggiunta all'introduzione di nuovo software, in modo che almeno i protocolli e l'accesso alla rete passino attraverso gli strati di software più recenti", ha aggiunto uno degli specialisti in sicurezza IT più anziani. Proprietari e operatori "devono ostacolare gli hacker con tutti i mezzi possibili".

"L'obiettivo (per proteggere rapidamente i sistemi SCADA) non dovrebbe necessariamente essere quello di contenere (o) sostituire tali sistemi, bensì di implementare tecnologie di blocco in grado di salvaguardarli il più possibile, oltre a seguire criteri più rigorosi per l'accettazione di nuovi sistemi in futuro."

I rischi SCADA sono aggravati dalle nuove piattaforme di distribuzione "intelligenti"

Le nuove piattaforme di distribuzione dei servizi, quali i sistemi interoperabili di "lettura intelligente" dei contatori dell'energia elettrica o di home banking su dispositivi portatili, creano nuove vulnerabilità ma offrono anche nuove opportunità. "La rete intelligente crea senz'altro nuove vulnerabilità, tuttavia ciò non significa che l'intero sistema energetico sarà più vulnerabile in futuro", ha affermato l'ex responsabile della sicurezza informatica del Dipartimento dell'Energia degli Stati Uniti Christopher "Rocky" Campione, aggiungendo che non si possono negare gli importanti vantaggi acquisiti in termini di maggiore efficienza e affidabilità.

Se poi i risparmi compensano i rischi, è ancora tutto da vedere. Una delle più importanti sfide che incombe sullo sviluppo della lettura intelligente è la capacità di mantenere i costi a un livello tale da permetterne l'adozione su larga scala. Le implicazioni di sicurezza di questa necessità sono allarmanti. "Quale livello di protezione è possibile integrare se il costo per unità non deve superare i cento dollari?" si è chiesto uno degli esperti.

"In un ambiente in rapida evoluzione, i responsabili IT e della sicurezza si trovano alle prese con calcoli sempre più difficili e informazioni limitate", ha dichiarato Campione. "È necessario prendere decisioni che tengano conto di opportunità, rischi e sicurezza, senza rimanere intrappolati nella "paralisi analitica". Non è possibile sapere tutto prima di prendere una decisione". In un simile contesto, non è quindi chiaro quanta attenzione sia stata prestata ai compromessi di sicurezza inerenti all'implementazione di "reti intelligenti".

Anche il cloud computing presenta nuove problematiche legate alla sicurezza

I sistemi cloud consentono alle aziende di affittare infrastrutture server e servizi software, in base a un'efficace strategia di outsourcing di tutti i requisiti informatici. A seconda del tipo di servizi e dati forniti in gestione, questo sistema può offrire nuove misure di sicurezza, così come creare nuove vulnerabilità.

Molti governi non riescono a risolvere la questione "organigramma" e, in alcuni casi, il risultato è un costante stato di lavori in corso.

Grazie al cloud computing infatti anche aziende di piccole dimensioni possono sfruttare tecnologie di sicurezza che altrimenti non si potrebbero permettere. Ciononostante, "il cloud computing mi terrorizza letteralmente", ha dichiarato uno specialista in sicurezza IT con una lunga esperienza alle spalle. "Non tanto perché sia a conoscenza di particolari problematiche legate a questa soluzione, ma piuttosto perché, storicamente parlando, ogni volta che ci siamo spostati in una nuova area non siamo riusciti a renderci conto delle nuove possibilità di attacco che si erano venute a creare".

"Stiamo tuttavia continuando a sviluppare sistemi progressivamente più complessi, il cui valore dipende sempre di più dalla capacità di fornire servizi ad altri sistemi che vengono connessi o autenticati in maniera approssimativa", ha concluso.

Secondo quanto afferma la Warren, per mitigare le vulnerabilità, aziende ed enti pubblici dovrebbero "valutare quali tipi di dati spostare nella cloud, nonché considerare il migliore modello di cloud per ogni tipo di business, analizzare attentamente il modello e le pratiche di sicurezza del service provider e definire linee guida per l'accountability dei servizi di hosting".

Necessità di una migliore organizzazione da parte dei governi per opporsi alle minacce cybercriminali

Un problema che è emerso più volte durante i colloqui con esperti di vari settori e paesi riguarda il modo in cui i governi si organizzano per affrontare le nuove minacce. Esistono dei modelli comuni; in tutti i paesi coinvolti, ad esempio, sono stati istituiti team di risposta alle emergenze informatiche (CERT, Computer Emergency Response Team) per la gestione della reazione agli eventi di sicurezza, anche se la loro efficacia non è omogenea, secondo quanto affermano gli intervistati. Tuttavia, molti governi non riescono a risolvere la questione "organigramma" e, in alcuni paesi, il risultato è un costante stato di lavori in corso.

In Brasile, ad esempio, il governo federale ha istituito nell'agosto del 2009 il Gruppo di lavoro per la sicurezza delle informazioni nella protezione delle infrastrutture critiche, nell'ambito del Dipartimento della sicurezza informatica e delle comunicazioni. Il gruppo di lavoro si occupa della sicurezza delle informazioni e della definizione di piani di reazione agli incidenti, secondo l'analista brasiliano Anchises de Paula di iDefense Labs.

In Australia, in un white paper sulla difesa del 2009 è stata annunciata l'istituzione di un centro operativo nazionale per la sicurezza informatica nell'ambito del Defense Signals Directorate (DSD) del settore militare, tuttavia molti dettagli restano ancora da definire.

Uno specialista australiano in sicurezza informatica ha dichiarato che il governo del suo paese ha investito un'enormità di tempo nello studio dei modelli britannici e statunitensi, così come di altri paesi, nell'ambito di una recente revisione dei propri criteri di sicurezza informatica. "Vi è una sorta di stallo tra la posizione di quegli elementi del governo che preferiscono il modello USA e quella di chi preferisce il modello britannico", ha dichiarato.

Poiché le infrastrutture critiche in molti paesi tendono a essere già regolate, questi cambiamenti possono creare difficoltà a proprietari e operatori con esigenze normative o di altra natura in conflitto o sovrapposte in relazione alla sicurezza informatica. I dirigenti si trovano spesso più a proprio agio con gli organi di controllo precedenti, mentre guardano con sospetto o preoccupazione ai requisiti normativi nuovi o aggiornati. Tuttavia, questi organi di controllo spesso non sono sufficientemente evoluti in materia di cybersicurezza.

Specialisti della sicurezza del settore idrico statunitense hanno affermato, ad esempio, di avere sempre avuto un ottimo rapporto con il proprio ente di controllo tradizionale, l'EPA (Environmental Protection Agency), tuttavia riconoscono come irrealizzabile la possibilità che lo stesso ente si occupi anche della regolamentazione della sicurezza informatica. "È impensabile che l'EPA assuma una qualsiasi forma di controllo normativo sull'infrastruttura informatica del paese", ha dichiarato uno di loro.

L'esistenza o la creazione di più agenzie con autorità normative, poteri investigativi o responsabilità di sicurezza nell'ambito della sicurezza informatica può anche dare adito ad attriti burocratici all'interno degli stessi governi.

Kimberly Zenz, ad esempio, ha dichiarato che i conflitti di competenza sul tema della sicurezza informatica si sono moltiplicati a Mosca. "Vi sono molte lotte intestine all'interno degli organi governativi russi. Si combatte a ogni livello. Tutte le organizzazioni federali, anche all'interno dello stesso ministero, sono ormai ai ferri corti".

Negli Stati Uniti, le frizioni nel ramo esecutivo vengono amplificate dai conflitti tra i comitati di supervisione all'interno del Congresso. "Il Campidoglio non ha alcuna competenza in materia di cybersicurezza a livello nazionale", ha dichiarato l'ex funzionario del Dipartimento dell'Energia Campione. "Si crea un effetto melassa", aggiunge, concludendo che la radice del problema sta nel modo in cui è organizzato il governo statunitense. "Se un legislatore (assegna dei fondi) alla sede centrale del CIO (di un'agenzia), il denaro finirà sicuramente a Washington o comunque sarà speso da qualcuno che sta a Washington. Se invece i fondi vengono assegnati a uno specifico ufficio (una qualunque sezione di un'agenzia), finiranno effettivamente in West Virginia... o a Pittsburgh o dove si vuole che arrivino", ha dichiarato Campione.

"I fattori che giustificano la spesa a Washington sono prevalentemente geografici". "Ecco perché", ha aggiunto, "tutti questi reparti governativi non sono in grado di consolidare la loro infrastruttura informatica".

La condivisione delle informazioni sembra funzionare meglio in senso orizzontale

I dirigenti hanno segnalato livelli di partecipazione più elevati all'interno di enti di condivisione delle informazioni di tipo orizzontale, da settore a settore, anche se nei vari paesi esistono strutture diverse per queste organizzazioni e livelli differenti di partecipazione.

La condivisione delle informazioni tra aziende che si occupano della sicurezza software, ad esempio, "ha fatto enormi progressi nel superare difficoltà a livello di proprietà (legge sulla proprietà intellettuale) e concorrenza", ha dichiarato Phyllis Schneck di McAfee. Schneck ha aggiunto che il settore "collabora molto bene... in particolare in questo periodo di crisi".

Un varietà di approcci ancora maggiore ha caratterizzato l'organizzazione dei forum di condivisione delle informazioni tra governi e settori industriali, con ampi divari nei tassi di partecipazione nazionali. Tuttavia, almeno nei dati del questionario, è possibile riscontrare una lamentela comune: i governi sono restii a condividere informazioni sensibili su minacce e vulnerabilità.

Il responsabile della sicurezza di un importante provider di telecomunicazioni ha dichiarato che la sua azienda ha rapporti con le forze dell'ordine di più di un centinaio di paesi in cui opera. Tuttavia, quando si tratta di condividere informazioni sulla sicurezza relative a infrastrutture critiche del paese, nessuno di essi "è in grado di fornirmi qualcosa di completo ed esauriente. Ciò che vorrei ottenere da un governo è qualcosa che non sarei in grado di procurarmi autonomamente: informazioni sulla natura delle minacce, che ci consentano di utilizzare meglio le nostre risorse, sulla base di un'analisi dei rischi più dettagliata di quella che potrei fornire io stesso. Sono loro ad avere in mano tutti i servizi di sicurezza e altre funzionalità".

Tuttavia, queste sono esattamente le informazioni che i governi tendono a salvaguardare più gelosamente, in parte perché non ritengono che vi sia un modo sicuro di condividere tali informazioni con proprietari e operatori di infrastrutture critiche senza rivelarle anche ai propri avversari.

Per questo motivo, livelli elevati di partecipazione in enti di condivisione delle informazioni gestiti dai governi non sembrano essere una buona strada verso il successo. Alcuni paesi adottano chiaramente strategie più esclusive nella condivisione delle informazioni rispetto ad altri.

Segretezza e sicurezza

"Negli Stati Uniti e in Europa si assiste a uno sforzo leggermente maggiore" nel condividere le informazioni da parte delle agenzie governative, ha affermato il responsabile della sicurezza, "tuttavia, quando si tratta ottenere informazioni veramente utili, ad esempio avvertenze o consigli sull'impiego delle risorse, non si riesce a portare a casa nulla, da nessun governo". Negli Stati Uniti, dove è stata segnalata una partecipazione superiore alla media a gruppi governativi di condivisione delle informazioni, si è tentato di superare l'ostacolo mediante l'assegnazione di autorizzazioni speciali a dirigenti di settori critici, ma i progressi sono stati incostanti.

"Solo a una o due persone (in una determinata azienda) viene assegnata un'autorizzazione", afferma Campione, "e a volte non si tratta delle persone giuste". Ha senso che l'autorizzazione venga assegnata a un dirigente anziano che potrebbe non avere le competenze tecniche necessarie per interpretare correttamente ciò che gli viene detto? Oppure che sia nelle mani di un dipendente tecnicamente più preparato, ma anche più giovane, che potrebbe quindi non disporre dell'autorità richiesta per gestire problemi che non può rivelare ad altri?

Un altro tipo di approccio, sostenuto da Pamela Warren di McAfee, consiste nel declassificare un numero maggiore di informazioni a un livello "sensibile ma non riservato", vale a dire "condivisibile tra membri di una community affidabile" che includa anche individui senza autorizzazione specifica. "Senza dubbio, parte del problema sta nel fatto che troppe informazioni vengono classificate come riservate", ha affermato l'ex funzionario del dipartimento dell'energia.

I dati indicano una collaborazione estremamente stretta tra settori industriali critici e governo in Cina.

In Australia, il dirigente responsabile della sicurezza Ajoy Ghosh ha dichiarato che il nuovo centro operativo nazionale per la sicurezza informatica avrà capacità operative e la possibilità di collaborare sul campo con proprietari e operatori di infrastrutture critiche. Negli Stati Uniti, invece, le agenzie governative hanno favorito una strategia basata prevalentemente sulla definizione di standard.

In Russia, secondo quanto afferma Zenz, il governo preferisce seguire un approccio più informale. Anche se non esiste una strategia informatica a livello nazionale e le indicazioni istituzionali in materia di condivisione delle informazioni o collaborazione sono estremamente scarse, i funzionari governativi "intrattengono relazioni molto strette con gli ISP... all'interno dei provider di servizi vi sono persone che hanno una consapevolezza di ciò che avviene nella rete in tempo reale" e che li tengono informati.

Una collaborazione estremamente stretta tra settori industriali e governo è rilevabile in Cina, dove i dati indicano elevati livelli di partecipazione e sostegno di iniziative di sicurezza guidate dal governo. Se tale collaborazione può essere replicata anche in altri ambiti è tuttavia ancora da dimostrare. Il generale Hayden ha tenuto a precisare che "si tratta di uno stato più autoritario rispetto agli altri, quindi potrebbe essere più facile... La popolazione forse... è più abituata a rispettare requisiti di sicurezza... considerati tutti gli aspetti della vita e della cultura cinese", oltre al fatto che l'uso di Internet, seppure diffuso e in continua crescita, è ancora limitato a una frazione molto selezionata della popolazione.

La difficoltà di collaborare in maniera efficace con i vari settori industriali è aggravata dalla natura totalmente instabile della minaccia. Come ha affermato uno specialista in sicurezza del settore dei trasporti statunitense, "Le competenze in ambito operativo si svalutano rapidamente (non appena un dirigente aziendale entra in contatto con gli) organi governativi. Questo è un problema particolarmente grave che le aziende si trovano ad affrontare ogni volta che si confrontano con le rispettive agenzie".

In effetti, lo stesso problema ostacola qualsiasi sforzo di coinvolgere il pubblico in un dialogo sulla sicurezza di tipo realistico. Il dibattito pubblico su problemi che riguardano la sicurezza presenta sempre delle problematiche che si fanno particolarmente acute in ambito informatico, sostiene il generale Hayden. "È sufficiente allontanarsi di uno o due passi dalla linea di partenza per lasciarsi il 95% degli ascoltatori alle spalle, tecnologicamente parlando... poi entrano in campo i sostenitori della privacy e la conversazione si fa improvvisamente molto complicata... Per noi gli ostacoli sono prevalentemente di tipo culturale".

Conclusioni

I dati raccolti con questa indagine indicano che le reti informatiche, in particolare quelle basate su IP, sono diventate di importanza fondamentale per proprietari e operatori di infrastrutture critiche. Nell'attuale clima economico, proprietari e operatori che impiegano la tecnologia per migliorare l'efficienza dei servizi che offrono dovranno affidarsi sempre di più alle reti, sia in ambito operativo che amministrativo. Dati e colloqui dimostrano che questi sistemi critici, inclusi quelli a carattere operativo come SCADA/ICS, operano in un ambiente ad alto rischio e si trovano ad affrontare un'ampia gamma di minacce, alcune delle quali potrebbero portare a conseguenze molto onerose. Tuttavia, i dati indicano anche che è possibile fare molto per proteggere questi sistemi, ad esempio mediante l'adozione su larga scala di misure di sicurezza chiave.

Se il cyberspazio è il Far West, allora lo sceriffo deve riportare l'ordine. I problemi di governance sono al centro di qualsiasi discussione sulla sicurezza di rete che coinvolga le infrastrutture critiche. Si sono registrati numerosissimi commenti, ad esempio, sulle barriere legali alla possibilità di utilizzare in modo più diffuso misure tecniche per neutralizzare gli attacchi DDoS. Gli esperti hanno inoltre discusso sulle difficoltà che si devono affrontare in fase di trattativa e degli altri sforzi in questo settore.

Per proprietari e operatori, l'indagine mostra come i rapporti con i governi siano un fattore chiave nella gestione della sicurezza. Per i governi invece tali rapporti sono cruciali per la difesa delle risorse nazionali. In assenza di una soluzione tecnologica che soddisfi tutti quanti, molti dirigenti vedono nei regolamenti normativi, malgrado gli svantaggi, un metodo efficace per migliorare la sicurezza. Oltre ai regolamenti, i dati indicano che in alcuni paesi, Cina in particolare, una stretta collaborazione tra governo e proprietari e operatori di infrastrutture critiche ha favorito il miglioramento delle condizioni di sicurezza.

Ringraziamenti

Mentre elaboravano l'enorme quantità di dati raccolta per questo report, gli autori e i ricercatori del CSIS hanno parlato in via formale e informale con decine di persone. Molti hanno accettato di essere intervistati e citati formalmente, altri hanno chiesto di non essere menzionati nemmeno nella sezione dei ringraziamenti, dove non esiste alcun nesso tra nomi e dichiarazioni. Siamo comunque grati a tutti coloro che ci hanno generosamente dedicato il loro tempo e hanno condiviso con noi le loro opinioni, indipendentemente dal fatto che il loro nome sia citato in questo report. Un ringraziamento speciale va a James Lewis per la sua consulenza e a Denise Zheng per averci aiutato a rispettare le scadenze del progetto. Ovviamente, gli autori si assumono la piena responsabilità per eventuali errori e omissioni.

Stewart Baker, distinguished visiting fellow, CSIS; partner, Steptoe & Johnson

Shaun Waterman, scrittore e ricercatore, CSIS

George Ivanov, ricercatore, CSIS

Michael Assante
vice president e chief security officer,
North American Electric Reliability Corporation

David Aucsmith
senior director, Microsoft Institute for
Advanced Technology in Governments

Christopher "Rocky" Campione
ex funzionario senior della sicurezza informatica,
Dipartimento dell'Energia degli Stati Uniti

John Carlson
senior vice president, BITS,
divisione della Financial Services Roundtable

Claudia Copeland
specialista di risorse e policy ambientali,
Congressional Research Service

Dan Corcoran
group information security officer, Consumer Group di Intuit

Kristen Dennison
analista di intelligence delle minacce, iDefense Labs

Ajoy Ghosh
security executive di Logica e docente di cybercrime
presso la University of Technology, Sydney

Gen. Michael Hayden (in pensione)
ex direttore, Central Intelligence Agency;
ex vicedirettore dell'intelligence nazionale;
ex direttore, Agenzia per la sicurezza nazionale

Rick Howard
direttore dell'intelligence di sicurezza, iDefense Labs

Aaron Levy
responsabile delle policy di sicurezza,
Association of Metropolitan Water Agencies

Anchises De Paula
analista di intelligence delle minacce, iDefense Labs, Brasile

Karl Rauscher
distinguished fellow, EastWest Institute; fellow, Bell Labs

Adam Rice
global chief security officer, Tata Communications

Phyllis Schneck
vicepresidente per l'intelligence delle minacce, McAfee; membro della commissione per la sicurezza informatica del CSIS per la presidenza Obama.

Paul Smocer
vice president, BITS, divisione della Financial Services Roundtable

Pamela Warren
stratega di cybercrime, direttore delle iniziative per il settore pubblico e le telecomunicazioni, McAfee

Tom Wills
Financial Services ISAC e iDefense Labs

Kimberly Zenz
analista di intelligence delle minacce, iDefense Labs

Note finali

1 L'indagine è stata condotta nel settembre del 2009 dalla società di ricerche di mercato Vanson Bourne, Ltd, con sede nel Regno Unito. Gli intervistati sono stati selezionati dagli elenchi di dirigenti IT che la società gestisce in vari settori e paesi per le proprie attività di ricerca. 100 delle 600 persone intervistate risiedevano negli Stati Uniti; 50 rispettivamente in Giappone, Cina, Germania, Francia, Regno Unito e Italia; 30 rispettivamente in Russia, Spagna, Australia, Brasile, Messico e India; 20 in Arabia Saudita. I settori maggiormente rappresentati sono stati quello bancario/finanziario e quello dei servizi governativi, con 145 intervistati ognuno. Il numero più ridotto di intervistati, solo 23 su 600, apparteneva al settore idrico/fognario. Gli altri settori (gaspetrolifero, energetico, trasporti e telecomunicazioni) sono stati rappresentati da un numero di intervistati compreso tra 59 e 82.

Considerando le dimensioni del campione, le conclusioni su modelli e variazioni sono state tratte a livello di settore e di paese, senza effettuare valutazioni sui vari settori all'interno dei singoli paesi.

Per le domande che riguardavano solo i responsabili di sistemi operativi (143 su un totale di 600 intervistati), le dimensioni del campione si riducono ulteriormente e anche le variazioni fra un paese e l'altro perdono di affidabilità. A questo riguardo sono stati inseriti dei commenti nelle sezioni del testo interessate.

In generale, nel corso delle interviste abbiamo cercato di sondare gli aspetti più sorprendenti e interessanti. Nei casi in cui i dati delle interviste sono risultati in contrasto con i dati dell'indagine, o ne hanno suggerito un'interpretazione differente, abbiamo aggiunto un commento esplicativo.

2 Alcuni aspetti dei dati dell'indagine russa si discostavano dalle informazioni emerse durante le interviste. Solo il 30% dei dirigenti russi ha riferito attacchi DDoS su larga scala, e solo il 3% di questi ha affermato di aver subito più attacchi mensili (la percentuale più bassa fra tutte le nazioni). "Gli attacchi DDoS sono un problema reale in Russia", ha dichiarato Kimberly Zenz, esperta di questioni russe di iDefense Labs, "gli attacchi colpiscono a 360°. Affittare una botnet in Russia è estremamente facile". Zenz ha affermato che gli attacchi ai siti web della concorrenza, perfino fra negozi di piccole città, erano all'ordine del giorno. Il settore dei servizi finanziari viene spesso colpito da attacchi DDoS e minacce di estorsione, ha aggiunto.

Questa apparente anomalia dei dati potrebbe essere in parte dovuta al modo in cui è stata formulata la domanda. Come esempi di attacchi su larga scala sono state usate le campagne DDoS contro Estonia e Georgia, attacchi di cui è stata ripetutamente incolpata la Russia. Questo potrebbe aver influenzato le risposte degli intervistati russi. Quando sono state poste domande sugli attacchi DDoS "di basso livello" (senza menzionare l'Estonia o la Georgia), il 73% degli intervistati russi ha riferito episodi di questo tipo, una percentuale molto più in linea con il totale degli intervistati, il 72% dei quali ha dichiarato di aver subito questo tipo di attacchi di basso livello.

Informazioni sugli autori

Stewart Baker è distinguished visiting fellow presso il Center for Strategic and International Studies e socio dello studio legale Steptoe & Johnson di Washington. Dal 2005 al 2009 è stato assistente segretario per la politica presso il Department of Homeland Security degli Stati Uniti. In precedenza aveva lavorato come consigliere generale per la Commissione Silverman-Robb, incaricata di indagare sugli errori dell'intelligence USA realtivamente alle armi di distruzione di massa irachene. Dal 1992 al 1994 è stato consigliere generale presso la National Security Agency.

Shaun Waterman è un giornalista e consulente sulle questioni del terrorismo e della sicurezza nazionale e interna, incaricato dal CSIS di occuparsi della ricerca e della redazione di questo rapporto. Attualmente lavora come reporter freelance per il Washington Times e altre pubblicazioni; dal 2000 al 2009 ha lavorato come corrispondente anziano e redattore presso la United Press International di Washington.

George Ivanov è un ricercatore del CSIS e candidato a una laurea specialistica in International Science and Technology Policy presso la George Washington University.

Per ulteriori informazioni sul CSIS, visitare: www.csis.org

Informazioni su McAfee

Con sede principale a Santa Clara, California, McAfee, Inc. è la principale azienda focalizzata sulle tecnologie di sicurezza. McAfee è costantemente impegnata ad affrontare le più difficili sfide legate alla sicurezza. L'azienda offre prodotti e servizi di sicurezza collaudati e proattivi che proteggono sistemi e reti in tutto il mondo, consentendo agli utenti di connettersi in modo sicuro a Internet, navigare ed effettuare acquisti sul Web in sicurezza. Supportata da un pluripremiato team di ricerca, McAfee crea prodotti innovativi destinati a utenti consumer, aziende, pubblica amministrazione e service provider che necessitano di conformarsi alle normative, proteggere i dati, prevenire le interruzioni dell'attività, individuare le vulnerabilità e monitorare e migliorare costantemente la propria sicurezza.

Per ulteriori informazioni, visitare il nostro sito web all'indirizzo: www.mcafee.com/it.

McAfee Srl
Via Fantoli 7
20138 Milano
Italia
(+39) 02 554171
www.mcafee.com/it

7795rpt_cip_0110