Dati rilevati dagli Enti certificatori o autocertificati
Tiratura: n.d.
Diffusione 10/2014: 400.000
Lettori Ed. II 2015: 352.000
Settimanale - Ed. nazionale

la Repubblica AFFARI&FINANZA

Dir. Resp.: Ezio Mauro

09-NOV-2015
da pag. 8
foglio 1 / 2
www.datastampa.it

A Chieti un server anti spie "Hacker a caccia di brevetti"

IL SISTEMA DI PROTEZIONE MESSO A PUNTO DALLA SELEX ES DI FINMECCANICA È IN GRADO DI MONITORARE GLI ATTACCHI IN TEMPO REALE MA IL PROBLEMA È CHE IL PRIMO FATTORE DI RISCHIO SONO I COMPORTAMENTI DI MANAGER, DIPENDENTI E PROFESSIONISTI

Luca Iezzi

Chieti

Benvenuti nel mondo delle guardie e ladri 2.0. Il cibercrimine ha abbandonato i mondi romantici e un po' lontani degli hacker geniali, degli attivisti politici, dei giochi tra spie per raggiungere le quello delle imprese anche quelle più piccole. I numeri sono impressionanti: secondo un sondaggio realizzato su migliaia di imprese Grant Thornton è arrivata a una stima prudenziale di circa 315 miliardi di dollari del valore economico dei danni prodotti nel mondo dalle intrusioni informatiche nelle aziende private, di questi 62 solo nell'Unione Europea. Inevitabile che crescano gli investimenti per prevenire queste minacce e non solo nel settore specifico dell'hi-tech o della finanza dove la sicurezza "occupa" già fino al 30% dei budget dell'Information technology.

Il mercato italiano della Cyber Security vale circa 2 miliardi di euro nel 2014 e si prevede arrivi ad un valore di circa 4,5 miliardi di euro nel 2024, con un tasso di crescita (cagr) del 7,8 %. Poco più del 50% è rappresentato da clienti governativi, militari e dal settore delle infrastructure critiche (Oil & Gas, trasporti, telecomunicazioni etc.), la restante quota è costituita dal settore privato. Selex Es, la controllata di Finmeccanica, specializzata nella difesa e nella sicurezza elettronica, sta sempre più spostando le sue competenze al servizio del settore privato. In pochi anni la stessa azienda che garantisce l'inviolabilità delle comunicazioni tra le varie basi Nato al di fuori degli Stati Uniti "difende" oltre 2500 clienti (aziende e pubbliche amministrazioni). «Serve un cambio di prospettiva - spiega Andrea Biraghi, managing director divisione information and security systems di Selex Es - ormai il 90% degli attacchi hanno motivazione economica, solo il 10% hanno finalità politiche o dimostrative. I casi frequenti sono la sottrazione di dati sensibili o rivendibili, o lo spionaggio industriale. In Italia esistono diversi obiettivi appetibili: piccole aziende che hanno brevetti importanti nel campo della manifattura, per non parlare delle grandi aziende che custodiscono i dati e la privacy dei propri clienti».

Un mondo criminale strutturato e segmentato, che prospera all'ombra di paesi con legislazioni molto benigne con chi usa la rete per violare la proprietà altrui, come l'Est europeo o l'Asia pacifica. Sul *deep web*, la parte di internet non indicizzate dai motori di ricerca, prosperano centinaia di mercati neri dove si possono comprare malware (i software che servono a intrufolarsi nei network), programmatori e capacità di calcolo, credenziali fasulle e informazioni riservate.

In questo senso l'informatica è solo un altro strumento in mano a ladri, intermediari, ricettatori comuni con minacce che arrivano da ogni dove, spesso via email. «La posta elettronica, lo spam, è uno dei mezzi più comuni con cui le infrastrutture informatiche vengono violate – spiega Biraghi – attraverso gli allegati, o rubando credenziali di persone interne alla struttura. Le incursioni a volte sono fatte su commissione, con un mandante e una vittima specifica, ma ci sono attacchi indistinti per procurarsi accessi alle aziende che possono essere "risvegliati" in un secondo momento».

Non esiste un antifurto infallibile, quindi il primo passo è un monitoraggio continuo, se possibile aiutato da potenti mezzi. Selex Es ha due centri di controllo principali a Chieti e a Bristol e i clienti vengono seguiti da remoto, la loro reti monitorate 24 ore su 24, le minacce e gli attacchi sventati con mezzi al di sopra delle capacità della singola azienda.

A Chieti un supercomputer tra i più potenti al mondo (32 mila cpu e 16 mila processori grafici) analizza le email e cerca di individuare gli eventi anomali prima che il vero e proprio attacco informatico porti alla distruzione o al trafugamento di dati. Il passo successivo è l'educazione di tutto il personale che deve seguire procedure formalizzate. «Il livello complessivo di sicurezza di un sistema è pari a quello del suo elemento più debole, per cui è inutile spendere per blindare una rete aziendale se poi i dipendenti portano i dati sensibili sui loro computer di casa o fanno entrare software non controllato in azienda attraverso le chiavette Usb». Non basta, sta crescendo la *cyber intelligence*: se gli attacchi hanno motivazioni economiche individuabili, una difesa avanzata è quella di fare controspionaggio, andando proprio a intercettare in anticipo i movimenti nel deep web mentre i criminali raccolgono informazioni e risorse per le proprie offensive. Livelli di difesa sofisticati accessibili a pochissimi.

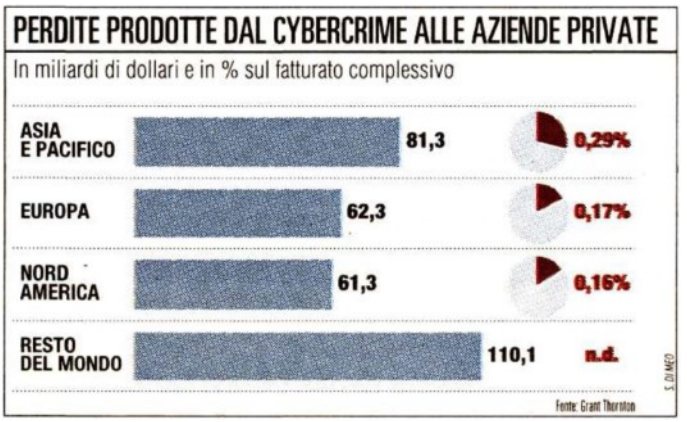
Secondo un sondaggio di Assoprim su 125 manager di aziende emerge che il 41% non ha mai considerato di adottare una strategia contro gli attacchi informatici, il 37% lo ha fatto solo nei limiti minimi imposti dalla legge, e di queste il 39% ha fatto tutto in casa senza avvalersi di consulenze professionali. «Bisogna avere un approccio differenziato, non tutti hanno bisogno di livelli alti, l'obiettivo è più semplice: definito il valore dei propri dati, bisogna rendere troppo costoso raggiungerli per gli eventuali assalitori esterni», suggerisce Biraghi.

Dati rilevati dagli Enti certificatori o autocertificati
Tiratura: n.d.
Diffusione 10/2014: 400.000
Lettori Ed. II 2015: 352.000
Settimanale - Ed. nazionale

la Repubblica AFFARI&FINANZA

Dir. Resp.: Ezio Mauro

09-NOV-2015
da pag. 8
foglio 2 / 2
www.datastampa.it



Andrea Biraghi managing director divisione information and security systems di Selex Es