Rapporto Clusit: nel 2017 (I semestre) reati informatici in aumento del 13% rispetto al 2016

DIFENDERSI DAL CYBERCRIME

Finanza e assicurazioni i settori più attaccati

DI LUCA RIGAMONDI

Se il 2016 è stato definito l'*annus horribilis* della cybersicurezza, il 2017 ha fatto segnare un nuovo record negativo: nel primo semestre dello scorso anno, infatti, gli attacchi gravi (cioè quelli che hanno avuto un impatto significativo in termini di danno economico, reputazione e diffusione di dati sensibili) di dominio pubblico sono aumentati dell'8,35% rispetto allo stesso periodo dell'anno precedente. Tanto che secondo il rapporto Clusit (l'Associazione italiana per la sicurezza informatica) diffuso a ottobre, «il primo semestre 2017 è stato complessivamente il peggiore di sempre in termini di evoluzione delle minacce "cyber" e dei relativi impatti, non solo dal punto di vista quantitativo ma anche e soprattutto da quello qualitativo». Il quadro che emerge dai dati è, secondo il report «disastroso» poiché siamo giunti a una condizione «di costante, quotidiano "allarme rosso", anche considerato che la tendenza generale, se il fenomeno non sarà contrastato con grandissima determinazione, è verso un ulteriore peggioramento».

Per quanto riguarda gli obiettivi, il Cybercrime (cioè i reati compiuti con l'obiettivo di estorcere denaro alle vittime, o di sottrarre informazioni per ricavarne denaro) è risultata la prima forma tra gli attacchi gravi, con 427 casi in crescita del 13,26% rispetto ai sei mesi precedenti. In aumento anche i crimini riferibili al Cyber Espionage (cioè lo spionaggio, 68 casi, +126%) mentre sono calati i casi di Hacktivism (cioè attacchi compiuti con finalità di attivismo digitale, 46 in totale nel primo semestre 2017, -41,03%) e di Information Warfare (guerra informatica, 30 casi nel 2017, -28,57%).

Rispetto al secondo semestre 2016, il rapporto Clusit sottolinea come la crescita percentuale maggiore di attacchi gravi si osserva verso la categoria dei cosiddetti *Multiple Targets* (+253,33%), cioè gli attacchi compiuti in parallelo dallo stesso attaccante contro numerose organizzazioni appartenenti a categorie differenti. Seguono i settori *Research/Education* (+138,10%) e Infrastrutture Critiche (+23,08%) seguite da *Banking/Finance* (+12,20%) e da produttori di hardware e software (+8%). Da segnalare la crescita (+16,67%) dei crimini informatici verso la categoria «Ricettività» (hotel, ristoranti, residence e collettività), che hanno tipicamente la finalità di colpirne i clienti finali. Cresce infine sensibilmente (+27,78%) la categoria «Altri», a ulteriore dimostrazione, sottolinea il rapporto, «che ormai tutti sono bersagli, a prescindere dalla dimensione e dal settore merceologico».

Per quanto riguarda specificamente l'Italia, i dati sugli attacchi (relativi al 2016) mostrano come a essere maggiormente presi di mira siano stati i settori «Finanza & Assicurazioni» e «Media» (entrambi al 22%), seguiti dal settore governativo (19%) e quindi dai provider di servizi (17%) e dall'e-commerce (11%). Proprio nel settore governativo italiano, sottolinea il report, è avvenuto uno dei 10 maggiori attacchi globali del 2016, «quello di matrice state-sponsored (forse originato dalla Russia) subìto dalla Farnesina, che avrebbe provocato la compromissione di alcuni sistemi non classificati». In generale, sottolinea **Andrea Zapparoli Manzoni**, membro del Comitato Direttivo Clusit, il salto della cyber-insicurezza nel 2017 è avvenuto «a fronte di investimenti in Sicurezza Ict ancora del tutto insufficienti rispetto al valore del mercato di beni e servizi Ict». Secondo l'esperto è quindi necessario «mettere a punto un nuovo modello di investimenti in Cyber Security, commisurandoli adeguatamente alle minacce attuali».

DISTRIBUZIONE DEGLI ATTACCHI PER TIPOLOGIA E TREND EVOLUTIVI

ATTACCANTI PER TIPOLOGIA	2011	2012	2013	2014	2015	2016	2H 2016	1H 2017	1H 2017 su 2016	Trend 2016
Cybercrime	170	633	609	526	684	751	377	427	13,26%	↑
Hacktivism	114	368	451	236	209	161	78	46	-41,03%	↓
Espionage / Sabotage	23	29	67	69	96	88	30	68	126,67%	↑
Information Walfare	14	43	25	42	23	50	42	30	-28,57%	↘
TOTALE	**469**	**1.183**	**1.152**	**873**	**1.012**	**1.050**	**527**	**571**	**+8,35%**	↗

Aggiornamenti costanti e più prudenza con le mail sospette
Le armi delle aziende per proteggersi dai virus

«Il software e le applicazioni da sole non bastano, spesso a causare la breccia nella security informatica è l'imprudenza o anche solo l'ingenuità delle persone»: a dirlo è **Federico Ziberna**, esperto di innovazione tecnologica attivo da molti anni come sviluppatore di sistemi informatici e cofounder nel 2000 di Emaze, società esperta in Cyber Security. «Le statistiche indicano che sono i ransomware mandati tramite e-mail ingannatorie e fraudolente a fare i danni maggiori: gli impiegati maldestramente cliccano e consentono ai software malevoli di impossessarsi del computer ospite e poi di dilagare nel sistema aziendale». Ziberna ha sviluppato un progetto-exploit sperimentale *NowISeeYou* per mostrare la banalità e anche le modalità subdole con cui avvengono la maggior parte degli attacchi informatici: «Abbiamo raccolto più di nove milioni di foto di avatar da WhatsApp e incrociando i dati con raccolti sui profili social, abbiamo dimostrato di poter risalire all'identità delle persone in maniera quasi certa. E questo perché le persone non sanno che anche le foto possono essere delle fonti di informazioni». Una miniera d'oro per malintenzionati che possono prenderle e rivenderle all'insaputa delle persone e con fini oscuri. «Banalmente, più attenzione e consapevolezza da parte di tutti consentirebbe di evitare molti problemi».

Federico Ziberna, cofounder di Emaze

Le nuove tendenze del settore? «Il nuovo paradigma *blockchain* sta cambiando tutto, consentendo scambio di informazioni e anche transazioni finanziarie tra due o più attori, validate dalla stessa rete decentralizzata dei peer. È una tecnologia che sembra più sicura, ma le aziende a breve dovranno capire come impiegarla e cambierà anche la percezione della sicurezza informatica attuale: è in atto un salto di paradigma con già un nuovo scenario alle porte». Ma il potenziale disruptive del cambiamento in atto non è solo qui. «All'ultimo World Summit di Lisbona, uno dei temi più discussi è stata l'affermazione dei sistemi di Intelligenza Artificiale che richiedono algoritmi sempre più sofisticati di apprendimento. Dopo il tema dei Big Data ci si è resi conto che il data mining (il sistema di estrazione di valore dai dati) dev'essere guidato dalle macchine, ma esteso ormai a tutti i supporti o i sistemi come la casa intelligente e l'auto a guida connessa: l'Internet delle Cose è un nuovo campo dove gli attacchi di nuova generazione stanno già avvenendo». La risposta anche qui è duplice, se da un lato servono sistemi di protezione sempre più basati sulle analisi predittive degli scenari criminosi, le macchine e gli algoritmi non possono fare tutto il lavoro da sole, vanno coadiuvate da esperti in grado di capire quando e come intervenire. In quest'ottica sono importanti per le aziende servizi di Ethical Hacking, come Penetration Testing e Sicurezza Applicativa che, utilizzati in maniera appropriata, consentono di prevenire i cyber crimini: occorre mettere in atto verifiche costanti dei livelli di sicurezza, e sviluppare un know-how adeguato per l'identificazione della vulnerabilità di sicurezza nel codice applicativo. E poi, visto che senza volerlo è spesso il personale interno alle aziende ad aprire le porte agli attacchi, non informato e non allineato con i principi di sicurezza, occorre organizzare campagne di consapevolezza mediante programmi di formazione sulla Cyber Security in ogni realtà lavorativa, pubblica e privata: «La risposta che va data è duplice, tecnologia sofisticata e all'avanguardia ma esperti e professionisti capaci di interpretarla e dipendenti resi edotti dei pericoli e sul come evitarli».

Michele Weiss

Bilanci positivi per tutti i segmenti del settore delle tecnologie per la sicurezza

UN MERCATO IN CRESCITA COSTANTE

La digitalizzazione degli edifici sospinge la domanda

DI LEONARDO RASTELLI

L'industria italiana fornitrice di tecnologie per la sicurezza e l'automazione degli edifici si conferma un comparto di eccellenza nell'ambito del made in Italy tecnologico. Il settore, rappresentato da Anie Sicurezza all'interno di Anie Federazione, raggruppa in sé gli operatori nel settore della sicurezza antincendio, antintrusione, TVCC, controllo accessi, building automation, ma comprende sempre più professionisti specializzati sulla Cyber Security.
Espressione a fine 2016 di un fatturato aggregato pari a 2,3 miliardi di euro, nel 2017 il settore nel suo complesso ha registrato una crescita del volume d'affari complessivo pari al 5,1%, in linea con quanto registrato in tutti gli ultimi anni. Il trend ha beneficiato sia della domanda di sicurezza sul fronte interno, sia delle strategie di rafforzamento delle imprese nei mercati esteri. Quale sia il valore rappresentato dalla Cyber Security in questi numeri è ancora difficile da descrivere, ma la digitalizzazione delle strutture, siano private o pubbliche, rende il segmento sempre più protagonista.


Giulio Iucci, presidente Anie Sicurezza

«La digitalizzazione implica la connessione di tutti i sistemi di security e safety», conferma **Giulio Iucci**, presidente di Anie Sicurezza, «quindi è evidente che laddove esiste la possibilità di un attacco esterno informatico, si richiede grande attenzione da parte di tutti i soggetti coinvolti. Ogni sito è sensibile agli attacchi cyber, in quanto i sistemi nel breve periodo saranno quasi tutti integrati fra di loro, per questo il tema della Cyber Security rigurada diversi mercati tecnologici: dall'energia all'industria, al building.È necessario lavorare insieme per portare la tecnologia al centro del processo di sicurezza, garantendo e pretendendo qualità su tutta la filiera: dalla risk analysis e risk assessment, al progetto esecutivo di un impianto; dalla produzione e distribuzione, alla installazione e manutenzione di un prodotto o di un sistema».
Non sorprende dunque che sull'onda delle nuove esigenze, dopo alcuni anni di flessione, a partire dal 2014 il sistema della sicurezza stia facendo registrare risultati positivi, con una crescita costante di circa il 5% anno su anno. Un risultato che attribuisce un ruolo sempre più rilevante all'industria italiana in ambito europeo. «L'Italia gioca un ruolo strategico in Europa», continua Iucci. «Non a caso ci piace parlare di made in Italy delle tecnologie, perché accanto alle tradizionali tre F (fashion, food e furniture, nda), esiste anche un'offerta tecnologica eccellente, che ci viene richiesta sia in ambito europeo che nei mercati extra Ue».
Tra i segmenti che registrano le performance migliori sia in termini di mercato che di evoluzione tecnologica, c'è, per esempio, quello della videosorveglianza. «Questo ambito va molto bene perchè, oltre a un forte upgrade tecnologico, ha elevato di molto la qualità media dei prodotti e beneficia di una domanda sempre crescente di sicurezza da parte dell'utente, anche privato cittadino. Basti pensare che il settore degli impianti di videosorveglianza negli ultimi 12 mesi è cresciuto del 10% e i sistemi antintrusione del 7.3%. Bene anche l'antincendio, che ha registrato un andamento sostanzialmente in linea con il 2016. Infine è cresciuto molto il settore dei sistemi audio di allarme vocale per l'evacuazione, spesso integrati proprio nelle offerte sul mercato con l'antincendio. In generale possiamo dire che è l'innovazione tecnologica la principale leva competitiva del comparto, che oggi trae nuova forza dalle molteplici possibilità offerte dalla digitalizzazione».

SICUREZZA E AUTOMAZIONE DEGLI EDIFICI

	2014	2015	2016	2015/2014	2016/2015
	milioni di euro			variazioni %	
MERCATO INTERNO	1.876	1.959	2.065	4,4	5,4
FATTURATO TOTALE	2.058	2.150	2.259	4,5	5,1
ESPORTAZIONI	290	330	345	13,9	4,6
IMPORTAZIONI	108	139	245	28,5	8,9
BILANCIA COMMERCIALE	181	191	194		

Fonte: ANIE - Source: ANIE

Industrial Cyber Security, la sfida si vince con la conoscenza

Tra le frequenti notizie di incidenti informatici che paralizzano le aziende, con danni economici sempre più ingenti, e l'emergere di nuove vulnerabilità che espongono al rischio di attacchi gli asset industriali, la Cyber Security sta rapidamente scalando i vertici delle priorità in molte imprese manifatturiere e sta uscendo dalle pertinenze esclusive dei reparti It per affermarsi all'attenzione dei manager di ogni settore, dalla produzione all'amministrazione, dalle risorse umane ai commerciali. A tutti loro è dedicato infatti l'**Ics (Industrial Cyber Security) Forum 2018**, la mostra-convegno organizzata da Messe Frankfurt Italia in collaborazione con Innovation Post, che si svolge oggi a Milano presso l'hotel Grand Visconti Palace. Oltre 500 gli iscritti, tra tecnici, manager e imprenditori che, in prima persona, si stanno aggiornando sull'aumento dei rischi e sulle possibili difese e che riceveranno da questa esperienza gli strumenti utili per valutare il proprio grado di maturità, conoscere gli aspetti normativi di maggiore rilevanza, capire come prevenire, riconoscere e reagire a un attacco. Concepito da un pool di esperti provenienti da aziende, università e istituzioni, il Forum, il cui sottotitolo è Cyber-smart manufacturing: cultura e tecnologie per l'industria connessa e protetta, prevede una prima sessione mattutina di introduzione al tema della Cyber Security all'interno di un percorso di digital transformation delle imprese manifatturiere. Seguiranno nel pomeriggio diverse tavole rotonde con le testimonianze di alcune imprese che hanno già iniziato ad affrontare il nodo della «governance» della sicurezza degli asset produttivi, tra cui Barilla, Enel, Saipem, Solvay, e diversi Workshop nei quali approfondire il funzionamento delle soluzioni commercialmente disponibili e ai quali aderiscono aziende come Siemens, Kaspersky, Fortinet o Servitecno.

Pietro Masotti

Tra gennaio 2016 e giugno 2017 l'Italia è stata raggiunta dal 2,53% dei ransomware mondiali

TROPPE AZIENDE ANCORA SENZA DIFESE

Pochi gli investimenti pluriennali e i professionisti della sicurezza

DI LEONARDO RASTELLI E GAETANO BELLONI

In Italia il mercato dell'information security sta crescendo, di pari passo con l'attenzione delle imprese tricolori nei confronti della sicurezza informatica. Tuttavia, il problema degli attacchi informatici – e quindi dell'efficace gestione della sicurezza e della privacy – è ancora un'emergenza che coinvolge privati, aziende, istituzioni e va affrontata a tutti i livelli. Un'analisi di Trend Micro, leader mondiale nella protezione dati in internet e la sicurezza nel cloud, ha rilevato che, tra gennaio 2016 e giugno 2017, l'Italia è stata raggiunta dal 2,53% di ransomware (un malware che limita l'accesso al dispositivo infettato, richiedendo un riscatto per rimuovere la limitazione) di tutto il mondo. Oltre 19 milioni i malware intercettati solo nel primo semestre dello scorso anno. Secondo una ricerca dell'Osservatorio Information Security & Privacy della School of Management del Politecnico di Milano, nel 2016 solo il 39% delle grandi imprese aveva un piano di investimento con orizzonte pluriennale, mentre il 46% includeva formalmente nel proprio organico la figura del chief information security officer, il profilo direzionale a capo della sicurezza». Il presidente del Consiglio Paolo Gentiloni, sul numero speciale della rivista *Gnosis* dello scorso novembre, dedicato proprio al decennale della riforma dell'intelligence, scriveva: «Si è operato per rimodulare in maniera radicale e innovativa l'architettura per la protezione cibernetica e la sicurezza informatica nazionali, che costituiscono precondizioni fondamentali per lo sviluppo del nostro Paese». Nell'occasione, il premier ha spiegato che: «Il decreto a mia firma è da considerarsi l'esito, sin qui culminante, di un processo riformatore snodatosi nel decennio, improntato a principi di coordinamento, raccordo, sinergia e collaborazione internazionale».

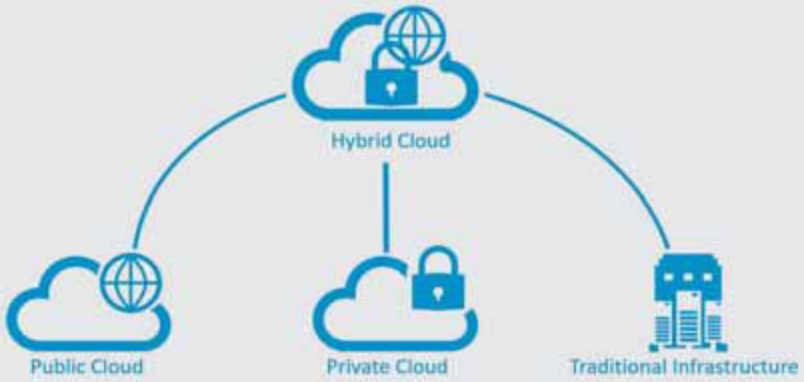
Fra i tanti contributi sul tema, a Milano si è svolto anche un workshop su «Nuove tecnologie e sicurezza: digitalizzazione, regolamentazione, frodi», organizzato da Experian, big player mondiale nei servizi informativi per la prevenzione dei rischi di credito e di frode, il marketing e la protezione dei dati di aziende e consumatori, e l'Associazione prestatori di servizi a pagamento (Apsp). Cuore del dibattito le questioni più urgenti da risolvere in tema di protezione dei consumatori dalle frodi nei pagamenti e le soluzioni più sicure contro il furto d'identità. «Simili tematiche sono di grande interesse per le aziende che, nel mercato digitalizzato, devono erogare servizi riducendo la complessità per il cliente senza aumentarne i rischi» ha sottolineato il presidente A.P.S.P. **Maurizio Pimpinella**. «Purtroppo però ancora troppe aziende hanno difficoltà ad adeguarsi a una normativa in continua evoluzione e sottostimano il rischio delle frodi. Si rende quindi sempre più necessaria la collaborazione di tutti gli operatori del settore: le competenze vanno messe a sistema e serve maggiore formazione per i professionisti e informazione per i consumatori perché, con la rapida evoluzione tecnologica, il rischio di incorrere in un digital gap è davvero dietro l'angolo». Secondo **Angelo Padovani**, amministratore delegato di Experian, le frodi si sono ormai industrializzate e il giro d'affari equivalente ha raggiunto il livello di mercato degli stupefacenti. «Il fenomeno è in costante aumento in tutto il mondo, facilitato da diversi fattori, primo fra tutti la multicanalità. I tradizionali modelli di scoring usati in area rischio di credito non sono in grado di intercettare adeguatamente i casi di frode, dato che i frodatori oggi sanno come superare certi controlli e sono in grado di presentarsi come buoni clienti, con determinate caratteristiche come un alto reddito o l'elevata anzianità lavorativa. Da un'analisi realizzata sul caso reale di un'azienda italiana è emerso per esempio che più del 50% dei clienti ad alto rischio frode presenta un rischio credito medio-basso». Ecco perché è sempre più urgente l'utilizzo di capacità analitiche avanzate, fondate sulla combinazione di tecniche diverse per la prevenzione delle frodi.

Device più robusti e nuove funzionalità, i progetti di Getac

I professionisti 3.0 hanno bisogno di *rugged* device, ovvero di tablet e computer robusti, progettati con hardware e software speciali adatti alla nuova era del Cloud. Le aziende hi-tech stanno lavorando per mettere a punto soluzioni affidabili e sicure anche nelle situazioni più estreme, con scocche rinforzate, funzionalità avanzate, e servizi pre e post vendita personalizzati. Getac è un produttore con esperienza decennale nella configurazione di device rugged; nei mesi scorsi ha lanciato, per esempio, il notebook semi rugged «S410» di ultima generazione, che stabilisce nuovi standard in termini di prestazioni, sicurezza multilayer e configurabilità. Con la sua versatilità, l'aspetto sottile e leggero, e le performance fra le migliori del comparto, l'ultimo S410 è lo strumento di lavoro ideale per i professionisti della pubblica sicurezza, la manifattura e per altre aree di servizi che operano sul campo. Una delle novità più significative è la videocamera IR opzionale che supporta il riconoscimento facciale con Windows Hello, per semplificare il login e aumentare la sicurezza. In combinazione con TPM 2.0 e SSD Opal 2.0, entrambi di serie sull'S410, offre agli utenti una soluzione mobile super sicura e utilizzabile in tutta tranquillità ovunque il lavoro li chiami. Getac è specializzato anche nel configurare sistemi professionali per clienti particolari, come Esercito Italiano, che hanno la sicurezza in cima alla lista delle priorità informatiche: «Oggigiorno le aziende sono più vulnerabili che mai al furto dei dati e agli attacchi», dichiara Rowina Lee, vice president of Global Sales & Business Development Centre di Getac. «Ecco perché Getac ha progettato l'S410, un pc in grado di supportare numerose funzioni di sicurezza integrate in Windows 10. PM 2.0 monitora e protegge gli avviamenti del sistema in modo da garantire che il dispositivo sia privo di manomissioni prima di lasciare il controllo al sistema operativo. BitLocker, invece, protegge i dati nei momenti di inattività, durante l'uso e in mobilità».

Michele Weiss

Vola l'Hybrid Cloud per la protezione dei dati



In tutto il mondo, Italia compresa, per la protezione dei dati si sta affermando il modello Hybrid Cloud. A confermarlo è anche l'Osservatorio Cloud & ICT as a Service della School of management del Politecnico di Milano, che in un recente rapporto ha attestato come il 17% degli investimenti sui cloud ibridi (ovvero a metà tra pubblico e privato) sia a supporto della cosiddetta «intelligence del dato», che identifica in servizi di protezione da Data Breach e da Cyber Attack una parte consistente degli investimenti.

Sono 160 i milioni di euro spesi dal nostro Paese per servizi Cloud based, e coincidono con l'imminente entrata in vigore del «Gdpr», il regolamento generale di protezione dei dati che dovrà venire applicato in tutti i Paesi Ue a partire dal 28 maggio del 2018. Secondo Alessandro Piva, direttore dell'Osservatorio, «in questa edizione si è visto che gli applicativi cloud usati dalle aziende sono in forte crescita, con un +36% sull'anno passato: ormai un'impresa su due adotta almeno una soluzione cloud, un segnale importante di fiducia nel sistema».

Michele Weiss

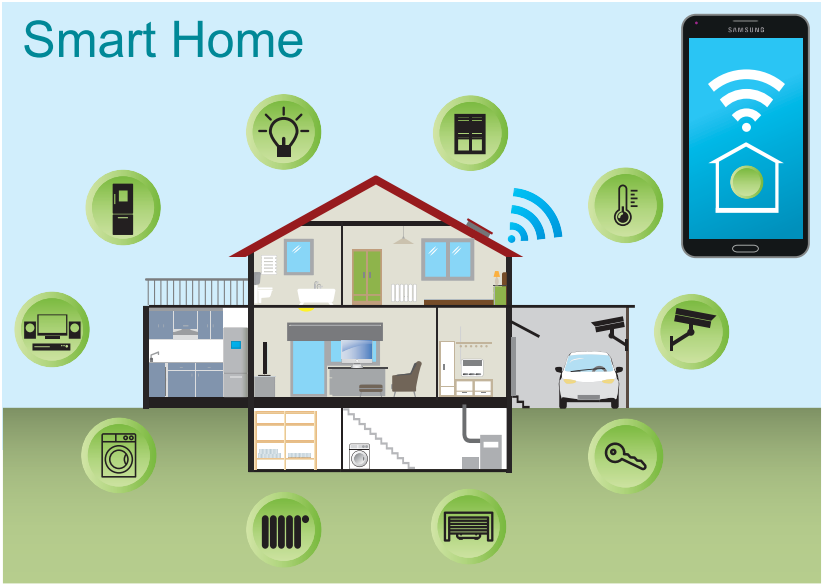
Ai malintenzionati basta un motore di ricerca per individuare i punti deboli della rete domestica

IoT IN CASA, PROTEZIONE O FALLA?

Nel mirino degli hacker router ed elettrodomestici connessi

DI ENRICO SBANDI

È un po' come sprangare balconi e finestre, attivare l'antifurto, ma poi uscire di casa lasciando le chiavi nella serratura. La metafora non è esagerata: gli strumenti connessi che sono ormai parte della nostra vita quotidiana sono altrettante potenziali vie d'accesso indebito alla rete da parte di malintenzionati. «Il rischio che qualcuno violi un nostro dispositivo Internet of Things è più alto di quanto si immagini», spiega **Simon Pietro Romano**, esperto di Cyber security e docente dell'Università Federico II di Napoli. «Che si tratti di una stampante, una videocamera o un elettrodomestico connesso, tutti questi dispositivi possono facilmente essere utilizzati da hacker per installare malware, creare una *botnet* con centinaia di migliaia di nodi o controllare attività che sfruttano la rete». Esiste persino un motore di ricerca dei dispositivi IoT connessi, accessibile a tutti: è www.shodan.io e permette di individuarli e selezionarli per tipologia e grado di protezione. Lo usano i ricercatori, i professionisti della sicurezza, e naturalmente anche gli hacker. Basta individuare una password di default, semplice da violare, e l'intrusione è fatta. «È anche un problema di alfabetizzazione», prosegue Romano. «È cruciale far capire all'utente finale quanto sia importante prestare attenzione ai punti deboli, perché la sicurezza è una lotta e chi è dall'altro lato è sveglio, ha tempo, voglia e soprattutto condivide informazioni; nella comunità degli hacker le informazioni circolano e circolano bene».



Con circa 6 miliardi di dispositivi nel mondo, l'Internet of Things fa gola ai cyber criminali. Videoregistratori digitali e telecamere IP sono i dispositivi oggetto degli attacchi più numerosi (63%); il 20% degli hacker ha nel mirino dispositivi di rete, come router e modem DSL (fonte: report Kaspersky Lab). Ma anche oggetti più tradizionali come auto e veicoli commerciali, se connessi, non sono risparmiati dagli attacchi informatici. La percentuale di veicoli con funzioni vitali (come le centraline di controllo del veicolo, dell'immobilizzatore e per lo sblocco del motore) legate alla rete è per ora limitata, ma con l'automazione della guida è un numero destinato ad aumentare esponenzialmente e a comprendere anche funzioni sempre più strategiche e fondamentali.

Nel dossier *Nuove modalità hi-tech dei furti d'auto*, realizzato da Lo Jack Italia, si evidenzia come già oggi questo ambito sia oggetto di un'aggressione diretta, mirata al furto, e a più stadi: prima viene introdotto il malware «di base» attraverso una comunicazione tramite rete cellulare o wi-fi che indirizza a un IP specifico e camuffato; una volta che l'applicazione è stata scaricata e installata, l'hacker prende il controllo del veicolo, ormai pronto a essere sbloccato e messo in moto.

LE SETTE REGOLE D'ORO ANTI-HACKER

Alcuni consigli semplici ma efficaci per difendere i propri dispositivi IoT da intrusioni moleste

1. **Dopo l'installazione, cambiare subito la password d'accesso, sostituendo quella di default**
2. **Cambiare periodicamente la password, evitando di usare la stessa per più dispositivi**
3. **Verificare tramite il sito della casa produttrice l'ultima versione disponibile del firmware del dispositivo e procedere all'aggiornamento.**
4. **Disattivare tutti i servizi di rete non strettamente necessari al funzionamento del dispositivo**
5. **Se la password standard non è modificabile o non è possibile disattivare l'account preimpostato, disabilitare i servizi di rete per cui sono impiegati**
6. **Evitare per quanto possibile di accedere al proprio dispositivo da una rete esterna o terza**
7. **Preferire i collegamenti via cavo alle connessioni wi-fi**

Difendersi (e fare business) col deep learning

«Nell'era dell'IoT, Machine Learning e Intelligenza Artificiale sono le armi impiegate su entrambi i fronti, lecito e illecito, per utilizzare le informazioni degli utenti». Secondo **Alessandro Livrea**, country manager di Akamai Italia, l'analisi e il controllo dei dati sul cloud è il nuovo fronte degli hacker mondiali, che utilizzano dei bot malware per penetrare nelle piattaforme web e impossessarsi di log, password e indirizzi mail degli account. Per questo occorre difendersi con la stessa tecnologia, il deep learning, per riconoscere e disinnescare le minacce: «Solo le aziende che sapranno evolversi potranno distinguersi e ottenere dei vantaggi competitivi sostanziali. Akamai offre ai clienti la possibilità di beneficiare di servizi di sicurezza basati sul deep learning, nonché di sfruttare degli algoritmi predittivi in grado di massimizzare il business». Con oltre 200 mila server in 130 Paesi, la piattaforma Akamai garantisce protezione dalle minacce informatiche con soluzioni per le web e mobile performance,

Alessandro Livrea, country manager Akamai Italia

la sicurezza sul cloud, l'accesso remoto alle applicazioni aziendali e la delivery di contenuti video. I dati indicano che nell'ultimo trimestre 2017, gli attacchi alle applicazioni web sono in aumento. In particolare, il Credential Stuffing - il furto delle credenziali sul web - è un grave problema per le aziende. «Inoltre, a fine maggio, entrerà in vigore il Regolamento europeo in materia di protezione dei dati personali, che rende le imprese responsabili delle informazioni sensibili dei clienti, con sanzioni molto pesanti», fa notare Livrea. Oggi le aziende si lamentano di non essere spesso a conoscenza degli attacchi, lanciati da bot invisibili: «Per questo noi abbiamo sviluppato soluzioni che usano il machine learning per disinnescare le minacce o per ribaltarle in vantaggi competitivi. Bot Manager Premier, per esempio, è progettato per aiutare le imprese online ad affrontare diversi tipi di attacchi bot nella maniera più veloce ed efficace possibile».

Michele Weiss

Se il pericolo arriva dall'aspirapolvere smart

Nell'era della *smart home*, nella quale ogni aspetto della casa, dall'illuminazione al riscaldamento, è gestito dalla rete, l'IoT mostra i suoi prodigi ma comincia anche a svelare le proprie falle. Per questo le aziende informatiche mondiali si applicano ogni giorno per testare i nuovi device connessi. L'israeliana Check Point Software Technologies, per esempio, ha verificato i protocolli sicurezza di alcuni elettrodomestici smart LG, tra cui Hom-Bot, l'aspirapolvere connesso wi-fi con microcamera integrata; ne è emerso che un bug consentirebbe a eventuali hacker di assumerne il controllo e utilizzarlo come talpa per un furto.

In realtà, la vulnerabilità risiede nell'applicazione per mobile e cloud LG SmartThinkQ, ma c'è da credere quello dell'azienda coreana non sia un caso isolato. Certo, trattandosi dei prodotti e del software di uno dei colossi dell'elettrodomestica mondiale, il fastidio non è di poco conto, visto che solo le vendite dell'Hom-Bot hanno toccato la cifra di 400mila pezzi solo nella prima metà dell'anno scorso (e sono 80 milioni i dispositivi smart home LG venduti nel mondo nel 2016). La storia, però, ha un lieto fine, visto che Check Point ha comunicato la criticità alla fine di luglio 2017, e alla fine di settembre LG ha rassicurato i consumatori comunicando di aver risolto il problema: »Una risposta di alto livello e immediata», ha confermato la software house israeliana. Ma, vien da chiedersi, è solo l'inizio?

Michele Weiss

http://www.milanofinanza.it - questa copia è concessa in licenza esclusiva all'utente 'IO099425' - http://www.italiaoggi.it

Lo specialista in scienze informatiche è tra le 10 professioni più difficili da reperire sul mercato

QUI SI FORMANO I SECURITY MANAGER

Aumentano corsi di laurea e master dedicati negli atenei italiani

DI ANDREA COLOMBO

Rispetto all'unica scelta obbligata che, soltanto fino a 15 anni, si poneva per uno studente che non avesse voluto prendere la strada dell'estero, oggi le possibilità di laurearsi in sicurezza informatica in un'università italiana sono molte. Il primo corso di laurea triennale in Sicurezza dei sistemi e delle Reti informatiche è datato 2003, e nasceva presso il polo di Crema dell'Università di Milano come una nuova specialità che permise di travasare nella didattica universitaria le competenze nate da una serie di progetti internazionali sulla sicurezza dei sistemi. Oggi lo stesso corso di laurea dell'ateneo milanese è proposto anche online, con il 90% del percorso di studio fruibile attraverso la piattaforma di e-learning, e il restante 10% in aule e laboratori della sede di Crema. Per chi poi non ha problemi con l'inglese c'è sempre la possibilità di seguire un corso in Cyber Security in un ateneo estero, anche online. Sono entrambi corsi di laurea che puntano a formare specialisti di progettazione, realizzazione, coordinamento e gestione di sistemi informatici nell'ambito della sicurezza e protezione dei sistemi, delle reti e delle infrastrutture informatiche, e al trattamento sicuro e riservato dei dati.

E che sia una laurea con un sicuro sbocco professionale di alto profilo è confermato dal mercato: lo specialista in scienze informatiche risulta in Italia tra le dieci professioni con maggior difficoltà di reperimento da parte delle imprese.

Sono otto le università in Italia patrocinate dal Laboratorio Nazionale di Cyber Security del Cini (Consorzio interuniversitario nazionale per l'informatica) che offrono corsi di laurea triennale e magistrale, corsi di specializzazione o di alta formazione, dottorati e master di primo e secondo livello in Cyber Security: la statale di Milano, appunto, il Politecnico di Milano, la Sapienza di Roma, l'Università Parthenope di Napoli, le Università di Genova, Pisa e Trento e l'Università degli studi di Modena e Reggio Emilia.

L'Università di Milano è l'unica a offrire un corso di laurea triennale (nelle due versioni), affiancato più di recente da un corso di laurea magistrale in Sicurezza informatica. Anche a Trento è possibile conseguire una laurea magistrale in Cyber Security nel Master EIT Digital Track, un corso organizzato in partnership con le Università di Twente (Olanda) e Turku (Finlandia).

Mentre tra gli atenei che non rientrano nel consorzio Cini vi è l'Università degli studi di Bari «Aldo Moro» con il suo corso di laurea magistrale in Sicurezza informatica.

Il Politecnico di Milano offre invece un Master di I livello (Alto Apprendistato «Security Specialist») e un Corso di Alta formazione di circa quattro mesi di durata (Information Security Management), la cui prima edizione risale al 2002.

Un altro corso di specializzazione è quello offerto dall'ateneo di Modena in Security Manager, della durata di 120 ore su tre mesi. In questa stessa sede sono attivi anche due Master di I livello: in Digital Forensics e Cyber Defense.

Altri Master di I livello sono organizzati dalla Sapienza di Roma (Sicurezza dei Sistemi e delle Reti Informatiche per l'Impresa e la Pubblica Amministrazione) e dall'Università di Pisa (Master in Cyber Security), mentre per i Master di II livello gli atenei da prendere in considerazione sono quello di Genova (Ciber Security and Data Protection) e ancora la Sapienza di Roma, che ne organizza ben tre: Governance e Audit dei Sistemi Informativi, Gestione della Sicurezza Informatica per l'Impresa e la Pubblica Amministrazione e Sicurezza delle Informazioni e informazione strategica.

Tecnici, ma non troppo Il perfetto manager Ict unisce hard e soft skills

«Cloud computing, soluzioni Open Source, evoluzione verso tecnologie real time e al contempo di Cybercrime prevention&prediction: queste sono le quattro macro-tendenze di mercato che stanno alimentando una forte richiesta di profili nel segmento del middle management». Mentre traccia lo scenario del settore, **Carlo Caporale**, amministratore delegato Italia di Wyser, società di Gi Group dedita alla ricerca e selezione di profili manageriali in ambito Ict, guarda anche ai profili più alti. «Anche ai ruoli più apicali si richiede oggi un buon equilibrio tra hard e soft skills, perché si devono conciliare il potenziale, la capacità e l'apertura mentale per gestire agilmente cambiamenti tecnologici e mutamenti di scenari».

Il mondo dell'industria 4.0, e soprattutto dei servizi di automazione, precision farming e agrifood, smart health, sicurezza e sorveglianza, richiede dunque nuovi professionisti Ict, che sappiano unire alle competenze tecniche anche qualità come flessibilità, propensione al lavoro in team e capacità di adattamento. Sono queste infatti le caratteristiche più richieste secondo l'analisi di Wyler, che segnala inoltre una crescita della domanda di persone con queste doti in maniera trasversale nei diversi ambiti della programmazione, delle infrastrutture, della gestione, della sicurezza e analisi dati, anche da parte di società di consulenza e piccole-medie software house che operano in ambito bancario/assicurativo.

Volendo tracciare un profilo completo, il professionista Ict deve avere: laurea in Informatica, Ingegneria Informatica, Gestionale o Elettronica, ma anche in Fisica, Matematica e Scienze Statistiche, una buona conoscenza dell'inglese sia per la gestione della documentazione tecnica che del rapporto con clienti e colleghi stranieri. Viene richiesta inoltre un'esperienza di almeno 3/4 anni per posizione, autonomia a livello tecnico e buona flessibilità trasversale in relazione ai diversi progetti e clienti di ogni singola realtà. «L'apprezzamento per background ed esperienze internazionali, nonché l'interesse a internalizzare competenze, sta portando molte realtà a offrire compensi davvero interessanti, capaci anche di attrarre professionisti italiani finora all'estero», sottolinea Caporale. A questo proposito nello studio Wyser la RAL (Retribuzione Annua Lorda) media offerta alle figure più ricercate tra Lombardia, Emilia-Romagna, Veneto e Piemonte, nei ruoli di Middle management, parte da una base di 35-45 mila euro per un Mobile developer, arriva a 40-55 mila euro per un DevOps Engineer, fino ai 65-70 mila euro per un Cloud architecht. Per quanto riguarda il Senior Management, il ruolo di Chief technical officer ha un guadagno che varia tra gli 80 e i 100 mila euro.

Accanto ad alcune figure più tradizionali, occorre evidenziare l'interesse delle società di consulenza in ambito finanziario per i Programmatori Full-Stack e Mobile, per lo sviluppo di nuove applicazioni utente. Caporale spiega come «sul doppio binario sicurezza/dati si vanno delineando le caratteristiche della figura professionale legata al nuovo Regolamento Europeo sulla Privacy, pienamente operativo da maggio 2018: il Data Protection Officer. Per rispondere al meglio alla compliance, il profilo ideale sarebbe quello di un esperto esterno all'azienda, con competenze giuridiche per l'interpretazione della norma, e informatiche per potersi rapportare adeguatamente con i responsabili dei sistemi informativi, ma capace inoltre di realizzare una completa analisi dei rischi connessi al trattamento dei dati e di valutare le interazioni con le altre discipline che riguardano, anche indirettamente, la sicurezza e la gestione delle informazioni». Anche in questo caso quindi si evidenzia la necessità di un profilo tecnico, ma non troppo, sicuramente molto agile e collaborativo, con competenze il più eterogenee possibili. Un aspetto quest'ultimo che, come fa notare anche Caporale, potrebbe facilitare la presenza e la valorizzazione di manager donne, in un ambiente invece per lo più ancora maschile.

Anna Carla Zucca

Carlo Caporale, a.d. di Wyser Italia