Jagriti Sinha (*)

IoT: la vera sfida è quella cyber

"IoT: una rete gigantesca che può contenere informazioni critiche e sensibili su qualsiasi individuo o realtà aziendale. Ed è ovvio che, con l'aumentare del numero di dispositivi connessi, la vulnerabilità agli attacchi informatici e alle intrusioni fraudolente nella rete IoT cresce anch'essa. Per ridurre al minimo i danni causati da tali attacchi e garantire un'adeguata sicurezza, sono state progettate soluzioni quali antivirus e antimalware. Pertanto, la crescita nel mercato della sicurezza dell'IoT può essere attribuita, per certi aspetti, al numero crescente di attacchi informatici come DDoS, ransomware e ingegneria sociale (studio del comportamento di una persona volta a carpire informazioni).

(*) Research Analyst, ICT Research, MarketsandMarkets Pvt. Ltd.
www.marketsandmarkets.com

Il ransomware è una minaccia incredibilmente dannosa, che può crittografare i file sensibili e bloccarli, a meno che non venga pagato un riscatto (ransom in inglese - ndR) per avere la chiave per la decrittazione.
Secondo l'Internet Security Threat Report del 2019, nel 2018 il volume complessivo degli attacchi IoT è rimasto elevato e coerente (-0,2%) rispetto al 2017. I router e le telecamere IP risultano i dispositivi più infetti e rappresentano rispettivamente il 75% e il 15% degli attacchi. Il che non sorprende, data la "congenita" accessibilità a Internet dei dispositivi in questione.

Il Cloud

Nel sistema IoT, invece, la maggior parte dei dati è archiviata nel cloud. Pertanto, anche se vengono crittografati, non ci sono ragioni per pagare un riscatto. Inoltre, se un hacker attacca un dispositivo, è facile ripristinarlo e instal-

Interviste raccolte dalla Redazione

Gianni Sabato

Titolare di Doing Security

“SERVONO SISTEMI A PROVA DI FUTURO. Grazie alle reti di ultima generazione e alla diffusione di apparecchi sempre connessi, l’IoT fa oggi parte del nostro quotidiano. Si tratta di dispositivi localizzati nel territorio che forniscono accesso ad utenti autorizzati, ne controllano l’operato e gestiscono impianti da remoto. Noi abbiamo applicato l’IoT ai contenitori di raccolta differenziata dei rifiuti sin dal 2000. Oggi sono disponibili molti più strumenti, rendendo più rapide ed efficienti la realizzazione e la diffusione dei dispositivi e consentendo di progettare funzionalità ‘a prova di futuro’. Le applicazioni spaziano dal controllo accessi in postazioni remote in totale assenza di reti cablate, all’uso delle isole ecologiche, Dalle colonnine di ricarica dei veicoli elettrici, al controllo remoto di parametri fisici”.

Raffaele Di Crosta

CEO Ksenia Security

“PAROLA D’ORDINE: DOMOTICA. Il mercato italiano dell’IoT è in crescita. Per le applicazioni, attualmente la parola chiave è domotica. Noi siamo impegnati nella ricerca di soluzioni a 360°, in grado di migliorare la qualità della vita e la sicurezza della casa, con un obiettivo ambizioso: la Smart Home. A mio avviso potrebbero dare maggiore impulso al mercato una migliore promozione da parte del distributore/installatore verso il cliente finale, che spesso non conosce le funzionalità domotiche di una centrale ed è erroneamente convinto che avere una casa domotica presenti un costo proibitivo”.

lare nuove patch. Inoltre i dispositivi IoT sono eterogenei, rendendo più impegnativo il “lavoro” degli hacker. Tuttavia, i cyber criminali stanno superando queste sfide, prendendo di mira il dispositivo giusto al momento e nel luogo giusti: ad esempio bloccando i termostati nelle fabbriche, quando sono alla massima temperatura.

Entro il 2023 avremo 44 miliardi di dispositivi connessi che genereranno zettabyte di dati, molti dei quali sensibili: la sicurezza è dunque la priorità

Home automation

Nella home automation, invece, gli hacker possono inviare una notifica quando il proprietario è in vacanza…scatenando il panico. E stessa cosa succede in determinati settori industriali, dove è possibile hackerare una rete elettrica o, in ambito sanitario, un frigorifero o un dispositivo biomedico di qualsiasi altro genere. Attacchi gravissimi, che portano i fornitori di soluzioni IoT a sviluppare strategie di sicurezza sempre più avanzate, che rappresentano quindi un vero e proprio elemento di traino per il mercato.

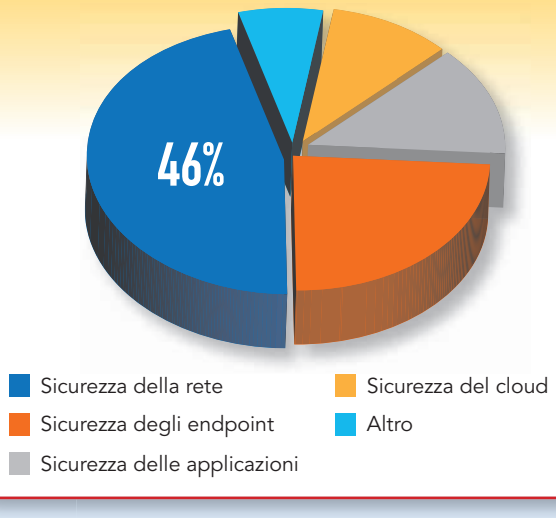
Un mercato in crescita

Il mercato della sicurezza IoT è in rapida crescita, a causa della crescente adozione delle tendenze Bring Your Own Device (BYOD) e della crescente domanda di

Luigi Giuliano
CEO Octopus IoT

"SERVE UN LINGUAGGIO DI COMUNICAZIONE STANDARD. L'IoT ha favorito la trasformazione tecnologica degli attuali modelli di business nel settore della security. La connessione tra dispositivi eterogenei è divenuto un elemento fondamentale della vita quotidiana del consumatore e le opportunità di sviluppo per l'IoT nel settore della sicurezza sono innumerevoli. Il comparto si muove verso l'integrazione dei sistemi eterogenei e il mercato è più ricettivo verso quelle tecnologie che integrano prodotti e servizi. Sicuramente un linguaggio di comunicazione standard favorirebbe la crescita delle tecnologie IoT e la competitività del mercato".

La sicurezza della rete domina il mercato della sicurezza IoT



tecnologie di cloud computing. Le soluzioni e i servizi di sicurezza IoT avanzati offrono una sicurezza completa per le applicazioni IoT e mantengono la riservatezza, l'integrità e la disponibilità dei dati trasferiti sui dispositivi IoT delle reti aziendali.

Sicurezza della rete

Come si può vedere dal grafico, l'esigenza di sicurezza di rete è quella più sentita dal mercato. Si tratta di una tecnica per proteggere le reti dalle minacce più avanzate raccogliendo e analizzando i diversi tipi di informazioni sugli eventi di sicurezza della rete. Rappresenta uno degli aspetti più importanti quando si tratta di proteggere l'ecosistema IoT. Consiste in comunicazione wireless, sicurezza dell'accesso remoto e gateway. La comunicazione wireless viene effettuata con l'aiuto di vari protocolli sicuri, tra cui LPWAN, Zig-Bee, 6LowPAN, Bluetooth, Z-Wave e NFC. Inoltre, l'antivirus e l'anti-spyware del gateway garantiscono la sicurezza IoT/M2M contro intrusioni, virus, spyware, worm, cavalli di Troia, adware, keylogger e Malicious Mobile Code (MMC) utilizzando meccanismi come ACL, sistemi di rilevamento/prevenzione delle intrusioni e filtraggio.

Comunicazione wireless

Nel mondo IoT, un'enorme quantità di dati viene comunicata tramite dispositivi remoti; pertanto la sicurezza di questa comunicazione wireless svolge un ruolo significativo nella sicurezza della rete. La tendenza chiave che contribuisce alla crescita del segmento di sicurezza della rete è proprio quindi la crescente adozione di applicazioni IoT tra vari settori.

Per saperne di più sull'indagine Industrial IoT Market by Device & Technology (Sensor, RFID, Industrial Robotics, DCS, Condition Monitoring, Smart Meter, Camera System, Networking Technology), Software (PLM, MES, SCADA), Vertical, and Geography - Global Forecast to 2023