ISABELLA CORRADINI
(A CURA DI)

FRANCOANGELI

INTERNET DELLE COSE

Dati, sicurezza e reputazione

REPUTATION AGENCY

Informazioni per il lettore

Questo file PDF è una versione gratuita di sole 20 pagine ed è leggibile con

La versione completa dell'e-book (a pagamento) è leggibile con Adobe Digital Editions. Per tutte le informazioni sulle condizioni dei nostri e-book (con quali dispositivi leggerli e quali funzioni sono consentite) consulta cliccando qui le nostre F.A.Q.

La reputazione di un qualunque soggetto è strettamente legata alla credibilità che il suo nome evoca. Essa è pertanto un fattore trainante per la determinazione del valore di un'azienda, un'istituzione o una persona. Vale a dire: **nel tuo nome il tuo valore**.

La reputazione nasce con le relazioni sociali ed assume un ruolo sempre più rilevante col diffondersi della tecnologia. Prima con la stampa, la radio e televisione, oggi con il web e i social network, rappresenta un fenomeno di immensa portata sociale e culturale.

Anche se le tecnologie hanno avuto ed hanno un importante ruolo operativo, le persone e i processi sociali restano centrali nel processo di costruzione e gestione della reputazione. Una reputazione ben gestita evita i rischi derivanti da una percezione negativa della propria immagine.

Questa *collana* intende affrontare il tema della reputazione attraverso una prospettiva multidisciplinare e facendo riferimento ad una varietà di contesti e di aree: il mondo aziendale nelle sue varie declinazioni, l'area della comunicazione con particolare riferimento agli attuali media, gli approcci di misurazione e di monitoraggio.

Un punto di riferimento fondamentale, dunque, sia per gli studiosi sia per gli operatori del settore.

ISABELLA CORRADINI
(A CURA DI)

INTERNET DELLE COSE

Dati, sicurezza e reputazione

FRANCOANGELI

Tutti gli indirizzi web indicati in questo libro sono stati verificati alla data della sua pubblicazione.

Indice

Premessa

di *Isabella Corradini*

L'Internet di domani sarà qualcosa di molto diverso da quello che attualmente conosciamo.

Si parla, infatti, di miliardi di oggetti che, dotati di sensori e connessi alla Rete, influenzeranno nei prossimi anni a venire gran parte dei settori lavorativi, dall'industria al commercio al sistema bancario, fino alle attività più private dell'individuo.

È l'"Internet delle cose", traduzione dall'espressione inglese "Internet of Things" (IoT), introdotta per la prima volta nel 1999 da Kevin Ashton[1] per descrivere lo scenario nel quale mondo fisico e virtuale si fondono. Una prima applicazione dell'IoT è riscontrabile già negli anni Ottanta, quando presso l'università americana Carnegie Mellon fu connesso ad Internet un distributore di bibite, in modo che il personale della struttura e gli studenti potessero controllare a distanza la disponibilità delle bevande. Con l'evoluzione di Internet, oggi le applicazioni possono essere le più diversificate. In questo contesto "intelligente" qualunque oggetto di uso quotidiano, come orologi, termostati, capi di vestiario, ecc., acquisisce – grazie ad un proprio indirizzo di rete – la capacità di ottenere ed elaborare dati dall'ambiente circostante e scambiarli con gli altri dispositivi.

È evidente che se cresce il numero di oggetti connessi ad Internet sono destinate ad aumentare anche le interazioni con chi li utilizza, ovvero i consumatori, determinando via via un ecosistema sempre più iperconnesso. Non a caso si parla già della naturale evoluzione

[1] Ingegnere inglese co-fondatore dell'Auto ID-Center al Massachussetts Institute of Technology (MIT).

dell'Internet delle cose verso l'"Internet di tutte le cose" (Internet of Everything, IoE), in cui l'interconnessione riguarderà dispositivi elettronici, persone, dati e processi.

La moltiplicazione dei dati prodotti da queste interazioni è un tema rilevante che apre diverse prospettive di analisi. Da un lato, infatti, l'Internet delle cose offre molteplici opportunità e vantaggi, considerato che i dispositivi elettronici, raggiungibili anche da remoto, offrono maggiori funzionalità da sfruttare nel quotidiano. Da notare che il mercato si va espandendo anche nella produzione di prodotti intelligenti particolarmente originali, dal materasso per monitorare il proprio sonno al calzino con il sensore, all'ombrello munito di connessione Wi-Fi.

Dall'altro però, espone a diversi rischi soprattutto per ciò che attiene alla protezione dei dati e alla sicurezza. Va da sé, quindi, che pur sottolineando i benefici che ne possono derivare, è bene fin da ora non sottovalutare i rischi, in modo da poter prevenire conseguenze che, come vedremo nel corso dei vari capitoli, vanno oltre il problema del "semplice" furto dei dati.

La questione di come tutti questi dati saranno utilizzati e protetti è cruciale nell'Internet delle cose. I sensori di cui sono dotati dispositivi e oggetti, infatti, raccolgono dati che riguardano abitudini e comportamenti delle persone: veri e propri profili reputazionali che potrebbero essere utilizzati per indirizzare attività commerciali e pubblicitarie mirate.

Molteplici, dunque, i temi che saranno approfonditi nei vari capitoli di questo libro: l'evoluzione dei sistemi ciber-fisici e l'importanza dell'analisi del rischio per prevenire le minacce dell'Internet delle cose (cap. 1); i comportamenti umani e le dinamiche di interazione tra individui e ambiente IoT, nonché la rilevanza del fattore umano nella gestione delle problematiche di sicurezza (cap. 2); le dimensioni economiche della privacy ed i comportamenti di acquisto, spesso guidati dalla scarsa consapevolezza del consumatore rispetto agli effetti della condivisione dei propri dati (cap. 3); il ruolo dell'identità digitale nel ridisegnare l'economia globale, il concetto di "Data protection by design and by default" nella nuova normativa europea della protezione dei dati e l'introduzione della tecnologia della

blockchain (cap. 4); esempi di usi IoT in ambito aziendale e analisi della relazione tra incidenti di sicurezza e reputazione del brand (cap. 5); l'approfondimento dell'Internet delle cose nel dominio dell'energia con la descrizione di alcuni progetti in ambito europeo (cap. 6).

L'obiettivo, quindi, è quello di fornire una visione multidisciplinare dell'Internet delle cose, integrando considerazioni di carattere tecnico, sociale, giuridico ed economico.

Pur nella diversità degli approcci impiegati dagli autori, la dimensione umana resta centrale: siamo nell'era dell'Internet delle cose, ma non si deve correre il rischio che siano gli esseri umani a diventare le cose di Internet.

1. Internet of Things e Cyber-Physical Systems: l'Internet delle cose insicure

di *Corrado Giustozzi*[*]

1. Dal cyberspace all'Internet delle cose

Quando nel 1982 William Gibson[1] inventò il concetto di "cyberspace"[2], egli stesso non aveva la benché minima idea di cosa potesse realmente essere: d'altronde a quell'epoca Internet era ancora molto al di là da venire, e lui non possedeva neppure un computer personale[3]. Così nella sua mente il cyberspace prese forma come «un'allucinazione vissuta consensualmente ogni giorno da miliardi di operatori legali, in ogni nazione, da bambini a cui vengono insegnati i concetti matematici... Una rappresentazione grafica di dati ricavati dai banchi di ogni computer del sistema umano. Impensabile complessità. Linee di luce allineate nel non-spazio della mente, ammassi e costellazioni di dati. Come le luci di una città, che si allontanano [...]». Insomma, un mondo virtuale fatto di informazione pura ed accessibile mediante tecniche di realtà virtuale.

[*] Consulente e docente di cybersecurity. Esperto di sicurezza cibernetica presso l'Agenzia per l'Italia Digitale per lo sviluppo del CERT della Pubblica Amministrazione, componente del Permanent Stakeholders' Group dell'Agenzia dell'Unione europea per la Sicurezza delle Reti e delle Informazioni (ENISA), componente del Consiglio direttivo di CLUSIT.

[1] Scrittore di fantascienza statunitense naturalizzato canadese, considerato il principale esponente della corrente letteraria cyberpunk.

[2] Comparso per la prima volta nel racconto *La notte che bruciammo Chrome* (*Burning Chrome*, 1982) e reso famoso dal romanzo *Neuromante* (*Neuromancer*, 1984).

[3] Un breve estratto di questo testo è stato pubblicato come contributo su *InterLex – Forum20* del 27 luglio 2017.

Oggi viviamo in una realtà più incredibile della fantascienza di trent'anni fa, e non ci facciamo nemmeno caso. Eppure interagiamo quotidianamente con una rete planetaria, Internet, che non solo è onnipresente ed ubiqua, ma è addirittura considerata un bene primario ed un diritto fondamentale; abbiamo tutti in tasca un dispositivo, lo smartphone, che unisce in sé funzioni di telefono, calcolatore, macchina fotografica, assistente personale... e ci offre l'accesso istantaneo a qualsiasi essere umano ed a qualsiasi informazione presenti sul pianeta; e gran parte della nostra vita sociale e di relazione la passiamo oramai nel ciberspazio.

Oggi inoltre tutto è "cyber", e questo già dà la misura di quanta acqua sia passata sotto i ponti da allora, in termini soprattutto concettuali oltre che meramente cronologici. Ed è piuttosto ironico che il termine cyberspace, nato per descrivere un incerto ed astratto concetto della fantascienza, sia stato sdoganato nel suo uso comune proprio da una categoria di persone considerate come assai concrete e quanto mai lontane dai voli pindarici della fantasia: i militari. Al giorno d'oggi, infatti, tutte le principali amministrazioni militari, compresa la NATO (Minárik, 2016), considerano ufficialmente il cyberspace come un "normale" dominio della conflittualità[4], ossia una dimensione materiale dove si applicano le leggi di diritto internazionale e possono aver luogo attività operative. Mentre i governi, dal canto loro, si preoccupano di adottare specifiche normative tecniche per innalzare la sicurezza del proprio "spazio cibernetico nazionale" contro le "minacce cyber". Il dominio cibernetico dunque non è più un'astrazione concettuale condivisa da un manipolo di nerd ma una vera e propria realtà oggettiva con una forte valenza pratica.

Ma se il mondo cyber di oggi è quello del post Internet, frutto cioè del boom della Rete negli anni successivi al 1995[5], probabilmente il bello deve ancora venire: e la rivoluzione pur epocale che ci ha tra-

[4] Per la precisione il cyberspace è comunemente definito come il "quinto dominio" del *warfare*, laddove gli altri quattro sono, cronologicamente: terra, mare, cielo e spazio.

[5] L'apertura agli utilizzi privati e commerciali della rete di ricerca ARPAnet, che sancisce di fatto la nascita di Internet, avviene nel 1990. L'invenzione del World Wide Web è di poco successiva, ma la sua diffusione inizia nel 1993 con la decisione del CERN di rendere disponibile a tutti il protocollo http e il linguaggio HTML che ne costituiscono le fondamenta.

ghettati dal mondo "prima-di-Internet" al mondo "dopo-Internet", verosimilmente impallidirà rispetto a quella che stiamo per vivere e che ci porterà al mondo degli oggetti connessi, alla cosiddetta "Internet delle cose" o, meglio, la "Internet di *tutte le cose*". Quello sì che sarà il definitivo spazio cibernetico del pianeta, dalla complessità davvero inimmaginabile. E se finora ci siamo lamentati della troppa rapidità con cui Internet è piombata nelle nostre vite e nella società, che non ha dato a quest'ultima il tempo fisiologico necessario a sviluppare una corretta maturazione culturale del fenomeno, con l'Internet delle cose (IoT[6]) la situazione sarà verosimilmente peggiore. Anche le stime più caute, infatti, prevedono che la velocità e l'ampiezza con cui si diffonderà l'utilizzo dei nuovi dispositivi "smart" faranno impallidire perfino quella, pur strabiliante, con cui si è sviluppata la stessa Internet.

Secondo un'analisi recentemente pubblicata da Intel[7], ad esempio, alla fine del 2017 il numero di dispositivi presenti su Internet sarà più del triplo del numero di abitanti sulla Terra, ed il traffico in Rete sarà cresciuto di tredici volte rispetto al volume di soli cinque anni prima. McAfee[8] invece stima che nel 2019 il traffico IP sulla Rete si aggirerà sui 168 Hexabyte[9] al mese, contro i circa 72 del 2015, e il numero di dispositivi connessi sarà di circa 25 miliardi.

È interessante notare, a questo proposito, che sin dall'introduzione del telefono il tasso di diffusione delle (nuove) tecnologie è andato sempre aumentando, ed il trend non sembra voler decrescere: ad esempio il tempo necessario per consolidare un bacino di cinquanta milioni di utenti nel mondo è stato di circa 75 anni per il telefono, 38 per la radio, 13 per la televisione e 4 per Internet: ma l'applicazione Angry Birds ha avuto 50 milioni di download in 35 giorni! Tutto ciò fa ritenere verosimili le stime di crescita del mercato dei dispositivi IoT, sia in termini di numerosità di apparati che di traffico generato sulla Rete. E se già oggi le comunicazioni *machine-to-machine* compongono una quota assai rilevante del traffico complessivo sulla Rete, in futuro con la capillare diffusione di oggetti "smart" e dispositi-

[6] In inglese: Internet of Things, abbreviato in IoT.
[7] *What happens in an Internet Minute?*, 2014.
[8] McAfee Labs, 2015.
[9] Un Hexabyte sono 10^{18} byte, ossia un miliardo di Gigabyte.

vi IoT il traffico fra umani sarà probabilmente quasi residuale rispetto a quello fra oggetti e dispositivi automatici.

L'avvento dell'Internet delle cose è la naturale conseguenza dello straordinario progresso tecnologico di questi ultimi anni, culminato in tempi recenti con la disponibilità di grandissime potenze di calcolo e di comunicazione a costi e con ingombri sempre minori. Oggigiorno, infatti, l'industria mette a disposizione dei progettisti chip che, pur costando pochi centesimi, offrono una capacità elaborativa superiore a quella di un grande computer di trent'anni fa e consentono una connessione wireless a banda larga secondo tre o quattro standard di comunicazione diversi. Ciò ovviamente consente e sempre più favorirà lo sviluppo e la produzione di una nuova e rivoluzionaria generazione di oggetti "smart", ossia capaci di svolgere in autonomia elaborazioni complesse e di comunicare in rete, nei più disparati settori, dall'elettronica di consumo ai veicoli ai sistemi industriali. Stiamo appena adesso iniziando a vedere sul mercato i primi elettrodomestici "intelligenti" (televisori, frigoriferi, aspirapolveri robot...) ma è chiaro che il fenomeno è inarrestabile, e soprattutto non sarà confinato solo al settore casalingo ma si estenderà ad ambiti quanto mai vari ed eterogenei. Il mondo dell'automobile ha già iniziato a parteciparne, e sarà rapidamente seguito da quello della domotica (tapparelle, porte, riscaldamento, illuminazione, sorveglianza...) anche per le inevitabili interazioni tra questi due ambienti, nei quali passiamo complessivamente la maggior parte del nostro tempo. I passi successivi saranno l'interazione con lo spazio urbano e tecnologico che ci circonda ("smart city"), con il nostro corpo (*wellness* e *fitness*), con gli altri (*infotainment*[10], *smart commerce*...). E non finirà di certo qui perché anche specifici ambiti specialistici, quali l'*healthcare*, si stanno già rapidamente orientando verso l'utilizzo di dispositivi medici personali in grado di interagire meglio e di più col paziente e con l'ambiente che lo circonda, oltre che con quello più propriamente diagnostico e clinico.

[10] Informazione spettacolo (o spettacolo dell'informazione).

2. I sistemi ciber-fisici

Con queste premesse è chiaro che il tema della sicurezza relativamente all'universo IoT diviene di straordinaria importanza per l'intera società. Anche perché questo mondo soffre purtroppo di una certa ingenuità progettuale sul tema, dovuta sia alla sua ancora acerba maturazione culturale sia alla velocità nel time to market imposta dalle logiche del business, per cui gli sviluppatori spesso non sono pienamente coscienti della natura e della portata del rischio e non inseriscono quindi nei prodotti delle adeguate funzionalità intrinseche di sicurezza. Il progettista di frigoriferi domestici o di lavatrici, ed esempio, non ha né la formazione specifica né l'esperienza maturata sul campo da un informatico che, da anni, è abituato a considerare e contrastare nei suoi prodotti i rischi di sicurezza ICT quali intrusione, sabotaggio, spionaggio, esfiltrazione di dati. Così è probabile che un "frigorifero connesso" non disporrà progettualmente di quelle contromisure di difesa che oramai il settore informatico considera tipiche ed irrinunciabili nei propri prodotti consumer, e costituirà quindi un *vulnus* straordinario nella rete casalinga, aprendola a minacce ed attacchi dall'esterno. E attenzione, non si tratta di ipotesi pessimistiche o di futuribili visioni apocalittiche, ma di fatti oramai già successi: le cronache annoverano infatti già da tempo casi di frigoriferi domestici compromessi da malware e utilizzati dalla criminalità organizzata per inviare spam in Rete[11], di televisori "smart" usati per catturare le conversazioni riservate che avvengono davanti alla loro telecamera[12], di telecamere di sorveglianza usate da malintenzionati per spiare le attività all'interno delle case dei loro proprietari[13], e così via.

Ma, almeno sul fronte delle nuove minacce al mondo cibernetico che ci circonda, non è finita qui. A fianco del mondo dell'IoT "puro", ma da esso non del tutto disgiunto, sta infatti giungendo a rapida maturazione un altro mondo tecnologico che, pur essendo altrettanto

[11] Si veda ad esempio: http://www.bbc.com/news/technology-25780908

[12] Si veda ad esempio: http://money.cnn.com/2015/02/09/technology/security/samsung-smart-tv-privacy/index.html

[13] Si veda ad esempio: http://gizmodo.com/a-creepy-website-is-streaming-from-73-000-private-secur-1655653510

importante e pervasivo, è stato considerato fino ad oggi come un universo a parte (per non dire che è stato addirittura obliato...), a causa delle sue specificità. È il mondo dei cosiddetti sistemi "ciber-fisici"[14], ossia di tutti quei sistemi di natura tipicamente industriale che, pur essendo dotati di una rilevante parte informatica, hanno come caratteristica principale quella di interagire in modo stretto e continuo con il sistema o l'ambiente fisico nel quale operano. Si tratta evidentemente di una classe di sistemi piuttosto ampia, che comprende sia oggetti noti da tempo come i sistemi SCADA[15] e le corrispondenti RTU[16], e più in generale tutti i sistemi relativi al controllo di processo in ambito industriale (ICS[17]), ma anche sistemi di natura sostanzialmente differente e di più recente introduzione quali quelli dedicati al controllo intelligente del traffico veicolare o ferroviario, i sistemi avionici posti a bordo dei moderni aeromobili, i sistemi di *healthcare* e trattamento clinico dei pazienti, i sistemi di domotica, i sistemi di interazione con l'ambiente urbano, e così via.

Le esigenze di sicurezza dei sistemi ciber-fisici sono particolarmente rilevanti in quanto ogni malfunzionamento o blocco della parte informatica comporta ovviamente effetti diretti sui sistemi fisici da essa controllati. Dunque i possibili impatti di un attacco deliberato, ad esempio di matrice terroristica o da parte della criminalità organizzata (che purtroppo non si possono più escludere), non si limitano alla semplice perdita o compromissione di informazioni ma possono comportare danni all'ambiente o alle persone e perfino il rischio di perdita di vite umane.

È importante a tal proposito notare come l'Agenzia dell'Unione europea per la cybersecurity (ENISA)[18], che tra l'altro redige un approfondito ed autorevolissimo rapporto annuale sul panorama delle minacce cibernetiche[19], abbia iniziato di recente a considerare i si-

[14] In inglese: *Cyber-Physical Systems*, abbreviato in CPS.

[15] *Supervisory Control and Data Acquisition* (Controllo di supervisione e acquisizione dati).

[16] *Remote Terminal Unit* (Unità terminale remota).

[17] *Industrial Control Systems* (Sistemi di controllo industriale).

[18] European Union Agency for Network and Information Security, https://www.enisa.europa.eu/

[19] *ETL-ENISA Threat Landscape*, https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/enisa-threat-landscape

stemi ciber-fisici come una categoria a sé stante, pur collocandoli concettualmente nell'ambito delle più ampie esigenze di protezione delle infrastrutture critiche. Inserendoli per la prima volta nella propria analisi riferita all'anno 2014, ENISA ha definito tali sistemi come «sistemi ingegnerizzati che interagiscono con apparecchiature di elaborazione, e vengono integrati in modo trasparente per controllare, gestire ed ottimizzare processi fisici in un'ampia varietà di aree della scienza ingegneristica tradizionale» riferendosi ad applicazioni nei campi della fornitura di energia, dei sistemi biomedicali per la cura e l'assistenza, dei sistemi industriali e di controllo della produzione, dei sistemi di trasporto, dei sistemi di telecomunicazione e di molti altri ancora.

In quanto collocati al confine tra gli ambiti della produzione fisica, della distribuzione e dei processi di sviluppo, i sistemi ciber-fisici risultano vitali non solo per gli aspetti di *security*[20] ma anche per quelli di *safety*[21], di privacy e di resilienza[22]. Costituendo tuttavia un settore relativamente nuovo e poco standardizzato, in termini ad esempio di mancanza di infrastrutture ed interfacce comuni, essi sono affetti da una elevata segmentazione delle soluzioni, le quali sono spesso assai specializzate per settori applicativi verticali. E, come accade più in generale per i dispositivi IoT, sono generalmente affetti da intrinseche carenze per quanto riguarda le misure di sicurezza.

3. Evoluzione delle esigenze di sicurezza

Perché anche questo mondo dei sistemi ciber-fisici, essendo più consolidato rispetto a quello dei dispositivi IoT e apparentemente più consapevole dei rischi, si trova invece nella medesima situazione di vulnerabilità? Innanzitutto per via della rapidissima penetrazione del-

[20] Intesa come protezione di beni materiali e/o immateriali oppure di servizi contro minacce tese a danneggiarli, comprometterli, manometterli, e comunque minarne il valore.

[21] Intesa come salvaguardia della salute, dell'incolumità e del benessere psicofisico delle persone.

[22] Intesa come capacità di continuare a svolgere la propria attività e/o erogare servizi assorbendo eventuali perturbazioni e superando incidenti che potrebbero ostacolare o compromettere il regolare corso delle operazioni.

le tecnologie ICT nel mondo dei controlli industriali avvenuta in questi ultimi anni. In passato i sistemi ICS erano governati da logiche di controllo realizzate ad hoc ed implementate mediante microcontrollori programmabili. Questi apparati avevano scarsissima potenza di calcolo e limitata capacità di comunicazione: attorno ad essi si sono sviluppati quindi dei protocolli di interfacciamento verso sensori ed attuatori estremamente semplici ed efficienti, dotati delle sole funzioni fondamentali, sia per facilità di implementazione e debugging che per le intrinseche limitazioni dell'hardware. Questo ha significato ad esempio l'assoluta assenza, nei protocolli di comunicazione e controllo fra sistemi, di concetti quali "utente", "autenticazione", "autorizzazione", i quali risultavano assolutamente non necessari nel contesto classico in cui tali sistemi operavano. Infatti, e questo è il secondo fattore rilevante, i sistemi di controllo industriale si sono sviluppati in un momento storico ed in un ambito operativo nei quali la sicurezza IT non li tangeva e non era considerata un rischio, essendo tutti gli apparati isolati dal mondo esterno non solo fisicamente ma, soprattutto, logicamente.

Lo sviluppo dei microcomputer prima, e dei computer personali dopo, ha tuttavia portato ben presto a sostituire molti degli apparati di controllo e supervisione passando da sistemi dedicati a sistemi basati su PC commerciali operanti con sistemi operativi standard, sui quali era ovviamente più facile sviluppare software. Successivamente la diffusione della connettività a basso costo basata sul protocollo TCP/IP ha portato a mettere in Rete tali apparati per facilitarne la gestione ed il controllo da remoto. Le reti di sistemi ICS sono dunque diventate a tutti gli effetti delle reti di sistemi ICT, con tutte le vulnerabilità di sicurezza di questi ultimi ma non le stesse difese. E con la differenza, rispetto al mondo puramente ICT, che sfruttandone le vulnerabilità non si ottengono solo effetti logici: compromettendo un sistema SCADA si possono aprire valvole, chiudere interruttori, attivare motori. Nel dominio dei sistemi ciber-fisici gli effetti di un attacco cibernetico si riflettono direttamente sul mondo fisico, e i danni sono reali, tangibili e potenzialmente spaventosi.

Ancora una volta questi timori per la fragilità complessiva dei sistemi di controllo industriale e, più in generale, di tutti i sistemi ciber-fisici, non sono solo teorici ma si basano su episodi preoccupanti che stanno già accadendo in numero considerevole. Il mondo delle

infrastrutture critiche tradizionali, infatti, sta già da tempo iniziando a risentire di problemi causati da minacce informatiche relativamente nuove per il settore, intenzionali o meno. Scoprendo tra l'altro che la principale e spesso unica misura da sempre adottata per la prevenzione contro gli incidenti, ossia l'isolamento delle reti, non sempre è sufficiente allo scopo.

Il caso sinora più clamoroso si è verificato alla fine di aprile del 2016, quando l'azienda elettrica tedesca RWE, che gestisce la centrale nucleare di Gundremmingen situata a circa 120 chilometri a nord-est di Monaco di Baviera, ha reso noto di aver rilevato del comune (e datato) malware su alcuni dei sistemi di controllo dell'impianto[23]. Si è trattato in effetti del primo caso noto di una centrale nucleare infettata da virus informatici, e come tale la notizia ha gettato una certa preoccupazione tra gli addetti ai lavori, anche se il regolare funzionamento dell'impianto non è mai stato messo realmente a repentaglio.

In particolare è accaduto che, su un sistema computerizzato di movimentazione delle barre di combustibile che nel 2008 era stato "retrofittato" con uno specifico software di visualizzazione di dati, sono stati trovati un virus, W32.Ramnit, risalente al 2010, e perfino un vecchio Conficker, risalente al 2008. In seguito alle prime indagini è apparso evidente che entrambi i virus erano residenti sui sistemi da parecchi anni, e dato che la rete interna della centrale non è connessa all'esterno vi devono essere stati portati mediante un utilizzo poco accorto di "chiavette" USB. Proprio questa mancanza di collegamento con Internet, per la cronaca, è il motivo per cui i virus non hanno fatto danni: in assenza di un centro di comando e controllo con cui poter comunicare, infatti, non hanno potuto svolgere i propri compiti e dunque sono rimasti inattivi. Inoltre altro malware è stato rinvenuto su 18 memorie di massa removibili, sia hard disk che memorie USB, usate in alcuni sistemi utilizzati per compiti amministrativi e di ufficio ed appartenenti ad una rete separata da quella di gestione dell'impianto nucleare.

Per quanto clamoroso, trattandosi di un impianto del genere, questo non è tuttavia il primo caso di impianto di produzione dell'ener-

[23] Si veda ad esempio: http://www.reuters.com/article/us-nuclearpower-cyber-germany-idUSKCN0XN2OS