Cybersecurity: conoscenza e consapevolezza come prerequisiti per l'amministrazione digitale

Pier Luca Montessoro

Il problema della cybersecurity è complesso e per comprendere i dettagli degli aspetti tecnici sono necessarie elevate competenze. Tuttavia, una efficace strategia di protezione dai rischi ad essa connessi si basa, prima che sulla tecnologia, sulla prevenzione guidata da conoscenza e consapevolezza. Questo articolo descrive gli aspetti fondamentali del problema evidenziando come tutti i soggetti coinvolti abbiano un ruolo e delle responsabilità, a partire dalla amministrazione che progetta ed eroga i servizi agli utenti finali che ne fruiscono.

1. *Cybersecurity*

Esistono numerose versioni della definizione di *cybersecurity*, non sempre coerenti e talvolta focalizzate su specifici aspetti del problema. Invece, nell'accezione più generale, la *cybersecurity* rappresenta una generalizzazione ed un'estensione del concetto di "sicurezza informatica". È interessante, per esempio, la definizione, disponibile *on-line*, che viene fornita dal dizionario Merriam-Webster: «*measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack*»[1]. Limitare il concetto alla sola protezione dei sistemi informatici è fuorviante e anacronistico. Estremamente più attuale e concreta è la definizione dello standard ISO/IEC 27032:2012[2] (rivisto e confermato nel 2018) che definisce la *cybersecurity*, ovvero la *cyberspace security*, come «*preservation of confidentiality, integrity and availability of information in the Cyberspace*». In questa definizione emergono due

(1) *https://www.merriam-webster.com/dictionary/cybersecurity.*

(2) ISO/IEC 27032:2012: *https://www.iso.org/standard/44375.html*: "Information technology – Security techniques – Guidelines for cybersecurity".

elementi chiave: *information*, perché l'obiettivo è quello di proteggere le informazioni (che spesso chiamiamo "dati", cioè informazioni convertite in forma digitale per essere elaborate, memorizzate o trasmesse), e *Cyberspace*, perché il contesto in cui agire per proteggere queste informazioni è infinitamente più complesso di un computer o della rete internet: «*Cyberspace: complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form*»[3]. Interazione tra persone, *software* e servizi. Ecco emergere il fattore umano, che diventa altrettanto importante quanto quello tecnologico. Ecco perché "conoscenza e consapevolezza", nel titolo. Anche se questa trattazione è focalizzata sull'amministrazione digitale e in particolare su come includere e affrontare il problema della *cybersecurity* nel processo di digitalizzazione della pubblica amministrazione, sarà presto evidente che questo problema è ormai pervasivo e interessa tutti, dal professionista esperto del settore al privato cittadino.

Il fatto che il tema della *cybersecurity* coinvolga in misura estremamente rilevante i comportamenti umani, e quindi la conoscenza e la consapevolezza che devono risiedere nelle persone, richiede che il processo di digitalizzazione della pubblica amministrazione sia accompagnato da opportune azioni strutturali di formazione per consentire ai cittadini digitali di muoversi nel nuovo mondo agevolmente e in sicurezza. Non esistono "nativi digitali". I giovani così etichettati dispongono di un'ottima manualità, sviluppata per tentativi e maturata come abitudine, nell'utilizzare i sistemi informatici, ma questo non implica affatto la conoscenza dei processi sottostanti e delle relative vulnerabilità. Se non esistesse il problema della *cybersecurity* questa conoscenza sarebbe in molte circostanze superflua, ma purtroppo il mondo reale è differente. Come sarà illustrato più avanti, il normale utente finale, anche se elemento periferico e apparentemente poco importante nel complesso sistema dei servizi digitali, rappresenta un appetibile punto di accesso per gli attacchi informatici da parte degli *hacker*[4], proprio perché meno consapevole dei rischi e più indifeso in termi-

---

(3) ISO/IEC 27032:2012, cit.

(4) L'uso del termine *"hacker"* richiede una precisazione. Nell'accezione più comune si riferi-

ni di sicurezza informatica. Anche per la *cybersecurity*, come per i vaccini, è necessaria la cosiddetta "immunità di gregge": solo una diffusa prevenzione basata sulla conoscenza può limitare significativamente la superficie di attacco e portare il rischio *cyber* al di sotto di livelli accettabili. Al pari di altri contesti ormai maturi, come la circolazione stradale regolata da opportuni codici, anche nell'utilizzo dei moderni servizi di rete deve maturare il concetto di responsabilità dell'utente nei confronti dell'intero sistema. Seppur importanti, le regolamentazioni in materia di *privacy*, trattamento dei dati, ecc., non trattano gli aspetti chiave in materia di linee guida per comportamenti sicuri. Inoltre, sia tali normative che quelle più orientate agli aspetti tecnologici quali quelle emanate dall'AGID (Agenzia per l'Italia digitale)[5] riguardano i gestori dei sistemi e i fornitori dei servizi e non i singoli dipendenti interni né gli utenti finali esterni.

La rapida evoluzione dei servizi digitali a disposizione dei cittadini è evidente e riguarda i settori più disparati. Una specifica direzione di questo sviluppo merita però una particolare attenzione perché dal punto di vista della sicurezza presenta alcune importanti peculiarità. Si tratta della *Internet of Things* (IOT), ovvero l'impiego nella rete internet di un gran numero di dispositivi che autonomamente acquisiscono informazioni e, interagendo con altri dispositivi e sistemi informatici connessi in rete, forniscono servizi agli esseri umani. Gli scenari più avveniristici mostrano veicoli a guida autonoma e frigoriferi che ci avvertono quando i prodotti alimentari contenuti sono prossimi alla scadenza e ordinano quelli mancanti, ma già adesso le telecamere di videosorveglianza, i sensori per il monitoraggio dei terreni nonché i sistemi di localizzazione presenti ne-

---

sce a qualcuno in grado di violare la sicurezza di un computer con scopi malevoli. Alcuni esempi: «To get into someone else's computer system without permission in order to find out information or do something illegal» (Cambridge Dictionary, *https://dictionary.cambridge.org/dictionary/*); «A person who uses computers to gain unauthorized access to data» (Oxford Dictionary, *https://en.oxforddictionaries.com/english*). Tuttavia, in origine il termine era associato a un movimento culturale orientato a superare creativamente i limiti imposti dai sistemi *software*, sia per sfida intellettuale che per democratizzare l'accesso all'informazione e superare i vincoli imposti dai sistemi "chiusi", le cui funzionalità sono definite esclusivamente dal produttore. Infatti, la comunità degli *hacker* ha successivamente coniato termini quali *"cracker"* e *"black hat hacker"*, con accezione negativa, e *"white hat hacker"* in senso positivo ("*hacker* etico" in italiano). Nel presente articolo, per semplicità, si utilizzerà il termine *"hacker"* nel senso di *"black hat hacker"*.

(5) *https://www.agid.gov.it/*.

gli *smartphone* forniscono concreti esempi di come potrà svilupparsi nel futuro la *Internet of Things*. Inoltre, gran parte della cosiddetta "industria 4.0" fa ampio uso di questa tecnologia. I dispositivi IOT si basano su computer estremamente piccoli ed economici, normalmente basati su sistemi operativi Linux, e saranno immersi nell'ambiente e presenti anche all'interno di prodotti non specificamente informatici. Questo porterà ad una enorme diffusione di oggetti che saranno la base per nuovi servizi ma anche obiettivi di attacchi informatici. Dal punto di vista della *cybersecurity* si presenta un nuovo aspetto del problema dovuto al fatto che i dispositivi stessi non sono direttamente accessibili e controllabili dall'utente, come invece è un normale computer. Quindi eventuali violazioni sono raramente evidenti e spesso impossibili da rilevare e soltanto interventi tecnici che prevedano l'accesso fisico al dispositivo possono ripristinarne in modo sicuro il normale funzionamento. In questo nuovo scenario la consapevolezza richiesta al cittadino cresce perché la criticità di questo nuovo paradigma è meno ovvia e spesso del tutto sconosciuta. Inoltre, molti dispositivi IOT sono destinati al grande pubblico mediante vendita diretta all'utente finale che si trova a doverli installare e configurare senza avere le conoscenze necessarie in materia di sicurezza.

2. *Portata del problema della cybersecurity*

Sarebbe fuori luogo riportare la lunga serie di numeri che raccontano quanto ampio sia il problema della *cybersecurity* e quali siano le conseguenze economiche e sociali. Per questo rimando ai numerosi report che vengono continuamente aggiornati ad opera di organismi nazionali e internazionali e società specializzate che operano nel campo della sicurezza. Alcuni riferimenti interessanti da cui partire: CLUSIT[6], Governo degli Stati Uniti[7], Symantec[8], Kasperky lab[9], Cisco[10]. Mi limiterò a un

(6) *https://clusit.it/rapporto-clusit/*.

(7) *https://www.whitehouse.gov/wp-content/uploads/2018/05/Cybersecurity-Risk-Determination-Report-FINAL_May-2018-Release.pdf*.

(8) *https://www.symantec.com/it/it/security-center/threat-report*.

(9) *https://ics.kaspersky.com/media/2018-Kaspersky-ICS-Whitepaper.pdf*.

(10) *https://www.cisco.com/c/en/us/products/security/security-reports.html#~2019%20Tbre-*

unico dato di estrema sintesi: in base a uno studio della rivista *Forbes*, il costo mondiale del *cybercrime* nel 2019 raggiungerà i 2.000 miliardi di dollari[11]. Tale valore è una frazione non trascurabile del PIL mondiale, che il Fondo monetario internazionale stima in 88.000 miliardi di dollari[12].

Ciononostante, l'aspetto economico non è il più rilevante. Questa vulnerabilità dei sistemi informatici rende fragili le innovazioni che si appoggiano su di essi. Nel passaggio al digitale si realizzano servizi (per esempio la PEC – Posta elettronica certificata) che sfruttano a loro volta altri servizi di supporto e infrastrutturali (*server* di posta, *data center*, servizi *cloud*, collegamenti di rete, sistemi di autenticazione degli utenti, ecc.). Purtroppo, in generale, i servizi sovrastanti non possono garantire livelli di sicurezza maggiori dei servizi su cui si appoggiano. L'esempio della PEC non è casuale. Nel novembre 2018 sono state violate circa 500.000 caselle PEC, incluse caselle di posta elettronica certificata di magistrati[13]. L'impianto normativo e giuridico relativo alla PEC assume che il sistema informatico funzioni, ma cosa accade se non si può più essere certi dell'identità dell'utente?

3. *Origine del problema della sicurezza*

Il problema della *cybersecurity* ha due profonde radici: la complessità e il già citato fattore umano. È interessante notare come le vulnerabilità del mondo digitale (o meglio, del mondo reale che si affida ai servizi del mondo digitale) derivino in parte da fattori tecnologici (complessità), in parte da comportamenti (fattore umano) e in parte dalla combinazione dei due (per esempio si sceglie una soluzione tecnologica meno sicura di un'altra perché più facile da utilizzare e quindi meglio accolta dall'utente). Nel seguito saranno analizzati gli aspetti fondamentali

---

at%20Report.

(11) *https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#4be2ceb53a91*.

(12) *https://www.imf.org/external/datamapper/NGDPD@WEO/OEMDC/ADVEC/WEOWORLD*.

(13) *https://www.adnkronos.com/fatti/cronaca/2018/11/19/mila-caselle-pec-colpite-attacco-hacker_8plKO45N4uAfUJ2QvNzboM.html*.

del fenomeno per poter successivamente delineare alcune linee guida per una efficace attività di prevenzione.

3.1. *Complessità e catena della fiducia*

I sistemi digitali sono estremamente complessi. Si basano su numerosi strati sovrapposti che aggregano funzioni semplici per ottenere funzionalità via via più sofisticate. Partendo da ciò che avviene nel dispositivo fisico (l'*hardware*), troviamo *transistor* e altri circuiti elettronici in cui si muovono gli elettroni, fibre ottiche in cui viaggiano i fotoni e antenne che generano e rilevano onde elettromagnetiche. Complesse reti di questi dispositivi permettono l'elaborazione e la trasmissione di segnali che, in forma digitale, rappresentano le informazioni. L'elaborazione di queste è definita dai programmi (il *software*), anch'essi estremamente complessi e suddivisi tra sistemi operativi, librerie, programmi applicativi, ecc.

Per avere un'idea di quanto elevata sia questa complessità si consideri che molte moderne CPU (*central processing unit*, il "cuore" di un computer, *tablet* o *smartphone*) sono composte da oltre mezzo miliardo di transistor; il sistema operativo *Windows 10* conta circa 50 milioni di linee di codice; i programmi di *Google* sono scritti in circa nove milioni di file per un totale di due miliardi di linee di codice. È evidente che tale complessità travalica i limiti del controllo diretto da parte dell'uomo. Non è solo questione di dimensioni ma anche di natura stessa dell'oggetto da controllare. Per verificare e interpretare cosa accade all'interno di un sistema digitale sono necessari altri dispositivi digitali e altri programmi. Così entra in gioco il concetto di fiducia, o meglio, di catena della fiducia.

Utilizzerò come esempio i sistemi di voto elettronico, che forniscono interessanti spunti di riflessione. Nei sistemi di voto tradizionale si supera il problema della (mancanza di) fiducia adottando procedure che permettono la verifica diretta – e in linea di principio attuabile da parte di chiunque – dell'esito della votazione, anche più volte e in tempi successivi mediante il semplice conteggio delle schede cartacee. La correttezza delle operazioni di voto (identificazione dell'elettore in modo che non possa votare più volte, consegna di una sola scheda, ecc.) è assicurata dalla presenza nel seggio di rappresentanti degli elettori (gli scrutatori). Al contrario, un sistema di voto elettronico richiede fiducia

in numerosi soggetti. Anche considerando solo gli elementi principali, troviamo i seguenti:

- l'elettore esprime il voto su un computer mediante uno specifico programma, quindi si dà fiducia in primo luogo a chi ha lo ha scritto: "registra davvero il mio voto?";
- l'autore del programma a sua volta ha dato fiducia a chi ha scritto il sistema operativo usato dal proprio calcolatore e chi ha prodotto tutti i sistemi di sviluppo da lui/lei utilizzati (in primo luogo il compilatore, che traduce il programma scritto dal programmatore in linguaggio sorgente, nella sequenza di codici binari eseguibili dalla Cpu che rappresentano le operazioni che davvero saranno svolte quando il programma sarà eseguito): "traduce fedelmente il programma e le intenzioni del programmatore?"
- chi mette in opera il programma di voto deve installarlo su tutti i computer dei seggi elettorali, quindi dando fiducia anche in questo caso ai produttori dei sistemi operativi e dei programmi necessari all'utilizzo di tali computer: "il computer su cui voto è sicuro?"
- il sistema di voto è poi basato inevitabilmente sulla raccolta dei voti mediante uno o più *database* centrali, i quali sono programmi (scritti da gruppi di programmatori – il che rimanda al primo punto della lista) a loro volta in esecuzione su computer con i relativi sistemi operativi: "dove finisce il mio voto?"
- affinché i voti vengano raccolti nei *database* è necessario che tutto il sistema sia collegato in rete, e quindi emerge il problema della fiducia in tutti i soggetti che hanno progettato, realizzato e gestiscono la rete: "come posso essere certo che il mio voto venga trasmesso correttamente?".

A tutto ciò si aggiunge il problema della potenziale insicurezza dell'*hardware*. Con la complessità che si è oggi raggiunta, è possibile nascondere all'interno delle Cpu degli ingegnosi circuiti elettronici composti da poche decine di *transistor* che consentono a un attaccante di prendere il controllo del sistema, anche se privo delle necessarie autorizzazioni[14]. Questo apre scenari inquietanti perché la produzione dell'*hardwa-*

(14) K. Yang, M. Hicks, Q. Dong, T. Austin, D. Sylvester, *A2: Analog Malicious Hardware*, in proc. 2016 Ieee Symposium on Security and Privacy (Sp), *https://ieeexplore.ieee.org/document/7546493*.

re è molto spesso demandata ad aziende esterne, situate per la maggior parte in estremo oriente, per cui la possibilità di controllo è pressoché nulla.

In condizioni normali, quindi, si dà fiducia a molte migliaia di soggetti (ripeto, considerando solo gli elementi principali) senza possibilità di un controllo diretto del funzionamento reale (e non solo apparente) del sistema. In più, esiste il concreto rischio di non trovarsi in condizioni normali. Per esempio, le elezioni rappresentano un bersaglio di grande interesse per gli attacchi *cyber*: se anche l'intero sistema fosse degno di totale fiducia, potrebbe comunque venire alterato intenzionalmente da soggetti terzi in modo da modificare a piacere l'esito del voto[15]. Esiste infatti l'ulteriore problema della vulnerabilità del *software*.

Anche se un programma è scritto da programmatori fidati utilizzando strumenti assolutamente sicuri, conterrà inevitabilmente delle criticità che possono essere classificate in due grandi famiglie: *bug* ("bachi", cioè errori di programmazione, non intenzionali) e limitata "robustezza" a fronte di dati di ingresso imprevisti (per esempio, sequenze più lunghe dello spazio di memoria dedicato a memorizzarle, formati difformi da quanto atteso, ecc.). Gli *hacker* investono ingenti risorse nella ricerca di tali elementi e nello studio di come possono essere sfruttati per modificare ad arte il comportamento del programma in modo da ottenere il controllo del calcolatore su cui viene eseguito. Purtroppo, il progettista deve correggere tutte le vulnerabilità del suo sistema mentre all'*hacker* basta scoprirne una, quindi il progettista viene inevitabilmente sconfitto[16].

---

(15) Nel corso degli anni si è assistito un vasto lavoro di ricerca, tutt'altro che concluso, per lo sviluppo di sistemi di voto elettronico verificabili. Per approfondire tale argomento un buon punto di partenza è: S.T. Ali, J. Murray, *An Overview of End-to-End Verifiable Voting Systems*, *https://arxiv.org/abs/1605.08554*. I numerosi modelli proposti spostano, senza mai annullarlo, il problema della fiducia. Per esempio, in alcuni di essi la verificabilità dipende dal comportamento degli altri elettori, in altri dal funzionamento (e dalla corretta implementazione) di algoritmi crittografici normalmente non comprensibili all'elettore. L'effettivo comportamento del sistema *hardware* e *software* per il conteggio finale dei voti resta in ogni caso uno degli elementi più critici in quanto raramente la verifica da parte degli elettori viene (dove tali sistemi sono già in uso) o verrebbe realmente attuata.

(16) M. Muller, *Iot Security: The Ugly Truth*, The Internet of Things Security Summit Talks 2015, Bletchley Park, *https://www.youtube.com/watch?v=j2qAkWDSDkg*.

In sintesi, è oggi indispensabile essere consapevoli del fatto che qualsiasi attività che si appoggi su servizi informatici e di rete si fonda su una catena di fiducia in numerosi soggetti in massima parte sconosciuti.

3.2. *Fattore umano*

Se quanto appena discusso può sembrare inquietante, è bene sapere che uno studio svolto nell'ambito del progetto europeo *Dogana*[17] ha rilevato che le vulnerabilità di tipo tecnico riguardano solo il 3% dei tentativi di attacco[18]. Il 97% è indirizzato a persone mediante tecniche di *social engineering*. Questo è davvero inquietante.

La *social engineering* è quell'insieme di tecniche che mirano a raggirare le persone, talvolta anche creando empatia e fiducia (malriposta) per indurre comportamenti che vanno a beneficio dell'attaccante. Non si tratta di un concetto nuovo, i truffatori esistono da ben prima dell'epoca digitale. Tuttavia, il mondo digitale mette a disposizione degli attaccanti nuovi strumenti che uniscono alla non tracciabilità delle proprie azioni la possibilità di automatizzare gli attacchi raggiungendo decine di milioni di bersagli contemporaneamente. Non è un caso se uno dei libri più noti nel settore della *cybersecurity* si intitoli "L'arte dell'inganno"[19].

Oggi tutti noi siamo costantemente oggetti di attacchi di *social engineering*. Per esempio, per quanto i sistemi automatici siano in grado di filtrare la maggior parte di messaggi di posta elettronica malevoli, un numero non trascurabile di mail di *phishing* raggiunge le nostre caselle di posta. Si tratta di messaggi che cercano di farci "abboccare" inducendoci, per esempio, a scaricare un *file* (contenente un virus) allegato al messaggio, oppure a collegarci ad un sito che riproduce l'aspetto del sito originale di un nostro fornitore di servizi ma che in realtà è stato sviluppato appositamente per sottrarci i nostri dati di autenticazione.

Negli ultimi anni gli attacchi di *social engineering* sono stati oggetto di una rapida e significativa evoluzione. Un esempio molto attuale è rap-

---

(17) *https://www.dogana-project.eu/*.

(18) E. Frumento, *Estimates of the number of Social Engineering based cyber-attacks into private or government organizations*, *https://www.dogana-project.eu/index.php/social-engineering-blog/11-social-engineering/94-estimates-of-social-engineering-attacks*.

(19) K.D. Mitnick, *L'arte dell'inganno*, Milano, Feltrinelli, 2003.

presentato dal crescente fenomeno detto *man-in-the-mail*, evoluzione del più generico attacco *man-in-the-middle*, in cui un attaccante si inserisce nella conversazione tra due interlocutori intercettandone ed eventualmente alterandone i messaggi. La versione più allarmante e dannosa è detta BEC, *Business Email Compromise*, e riguarda, come suggerisce il nome, la posta elettronica di aziende ed enti commerciali. Tale tipologia di attacco evidenzia bene anche il ruolo chiave della sicurezza del dispositivo dell'utente finale e dell'importanza della sua corretta gestione. L'attaccante ottiene il controllo del computer o dello *smartphone* di un responsabile amministrativo di un'azienda o di un ente. Questa prima fase è più semplice di quanto possa apparire perché, anche se in alcune circostanze l'attaccante si prefigge uno specifico obiettivo, molto più spesso procede in senso inverso, limitandosi a selezionare, tra le migliaia di dispositivi che è riuscito a infettare, quelli che contengono messaggi di natura amministrativa. L'accesso ai messaggi di posta elettronica può essere stato ottenuto, per esempio, mediante i *malware* (*software* malevolo, per esempio i cosiddetti virus) diffusi tramite messaggi di *phishing* con la posta elettronica o nascosti in *app* per *smartphone* scaricati da utenti ignari della loro pericolosità. L'attaccante è così in grado di analizzare gli scambi di messaggi, spesso piuttosto ripetitivi, che regolano specifici aspetti amministrativi dei rapporti commerciali, per esempio le comunicazioni delle coordinate bancarie verso istituti esteri. Può così intromettersi in una consueta comunicazione e alterare un messaggio o forgiarne uno *ex novo* a suo beneficio (per esempio modificando le coordinate bancarie) senza che il destinatario si insospettisca perché quanto ricevuto è del tutto coerente con la procedura in corso (che l'attaccante ha avuto modo di imparare). Secondo un'indagine dell'ente governativo americano FBI, tra il 2013 e il 2018 il BEC ha fruttato ai criminali informatici 12 miliardi di dollari[20].

La tipologia di attacco che BEC rappresenta mette in evidenza due importanti criticità, entrambe dipendenti dai comportamenti umani: la vulnerabilità causata da una incauta gestione dei dispositivi e la vulnerabilità causata da procedure che ripongono troppa fiducia nell'affidabilità

(20) *https://www.ic3.gov/media/2018/180712.aspx*.

dei dati scambiati in rete. Per quanto riguarda i dispositivi, la semplificazione delle modalità di configurazione e di utilizzo dei sistemi operativi e dei programmi applicativi ha spostato la responsabilità della loro gestione tecnica dai sistemisti esperti, che una volta erano gli unici soggetti autorizzati a (e in grado di) installare e configurare i sistemi informatici, agli utenti finali, anche se totalmente inesperti. Questo ha permesso una rapida diffusione di *malware* anche in assenza di vulnerabilità sul piano tecnico. Per esempio, quando si installa una *app* sul proprio *smartphone* è necessario concedere esplicitamente delle autorizzazioni per l'accesso a informazioni e funzionalità del dispositivo. Troppo spesso queste autorizzazioni vengono concesse senza interrogarsi minimamente sul grado di fiducia che sarebbe ragionevole dare al loro sviluppatore (tipicamente sconosciuto). Così, si installa un programma per utilizzare il *flash* della macchina fotografica come una torcia e gli si fornisce l'accesso ai dati sulle chiamate, ai messaggi, alla rete[21]. Se nel dispositivo transitano informazioni sensibili, quali i messaggi della posta elettronica aziendale, si apre una pericolosa breccia nella sicurezza dell'intera azienda. Infatti, la linea di condotta detta BOYD (*Bring Your Own Device*), cioè l'utilizzo dei dispositivi personali per attività aziendali, è molto dibattuta. Se da un lato essa consente risparmi (il costo del dispositivo è a carico del dipendente) e maggior produttività (trattandosi di un dispositivo personale è molto probabile che il dipendente lo porti sempre con sé e quindi sia sempre raggiungibile), d'altra parte espone maggiormente l'azienda ad attacchi informatici. Va anche considerato il fatto che i dispositivi personali possono portare all'interno della rete aziendale, e quindi oltre le barriere tecnologiche poste a protezione della rete interna[22], virus e *malware*[23] in grado di aprire le porte ad accessi non autorizzati dall'esterno e di attaccare i sistemi critici, per

(21) È molto istruttivo leggere le autorizzazioni richieste dai più popolari programmi "*torch*" disponibili su *Google Play Store*.

(22) Per esempio i *firewall*, dispositivi che controllano e filtrano il traffico di rete.

(23) A questo proposito va citato il problema della scarsa conoscenza dei rischi conseguenti l'accesso a siti *web* illegali (per esempio siti pirata di *video streaming*) o l'utilizzo di copie illegali di programmi; in entrambi i casi si espone il proprio dispositivo a numerosi e pericolosi *malware* che successivamente possono attaccare la rete aziendale.

esempio i server contenenti i dati dell'azienda. La seconda criticità deriva dalla mancanza di consapevolezza di quanto i sistemi digitali siano vulnerabili ed espongano i loro utenti a rischi ed attacchi informatici. La posta elettronica non fornisce garanzie sull'autenticità del mittente né del contenuto dei messaggi (dovrebbe farlo la PEC, salvo attacchi quali quello citato al punto 2). Di conseguenza, definire procedure operative critiche come trasferimenti di denaro basate esclusivamente su informazioni scambiate tramite posta elettronica è rischioso e concettualmente sbagliato. Per questo la conoscenza e la consapevolezza sono assolutamente essenziali per poter valutare correttamente l'impatto delle scelte operative nella progettazione, realizzazione e gestione dei servizi, soprattutto nell'ambito della pubblica amministrazione e ancora di più quando questi coinvolgono direttamente i cittadini.

3.3. *Criminalità organizzata*

Nel 1983 il film *WarGames* fece conoscere al grande pubblico il problema della *cybersecurity* nel contesto dell'epoca, quando molti erano gli *hacker* che cercavano di violare i sistemi più per gioco (il protagonista del film è un ragazzino) o per sfida intellettuale, piuttosto che per trarne profitto. Lo scenario è cambiato radicalmente. Oggi gli strumenti tecnici per sferrare attacchi informatici sono in vendita sul cosiddetto *black market*[24] del *dark web*[25] e di conseguenza il crimine informatico può essere perpetrato anche da soggetti non particolarmente esperti delle tecnologie. Tutto questo ha portato allo sviluppo di una vera e propria criminalità organizzata che fa ingenti profitti tramite le diverse forme di crimine informatico.

È interessante notare come le attività della criminalità informatica si spostino nel tempo per massimizzare i profitti e minimizzare i rischi. Questo risulta molto evidente analizzando come nel corso degli anni cambiano i dati contenuti nei già citati report sulla *cybersecurity*. Per esempio, nell'ultimo anno (2018) si è assistito a un calo di alcune fami-

---

(24) Mercato *on-line* di prodotti e servizi illegali.

(25) Una porzione del *web* che è nascosta ai normali motori di ricerca e che non è accessibile tramite i normali strumenti di navigazione in rete in quanto fa uso di opportuni protocolli per garantire l'anonimato.

glie di *malware* e un forte incremento di quelle legate agli scenari più nuovi e innovativi: crittovalute e *Internet of Things*[26].
Le crittovalute sono dei sistemi monetari non ufficiali[27] privi di un'autorità centrale; basandosi su tecniche crittografiche avanzate registrano le informazioni relative alle transazioni in modo non modificabile[28] su un registro pubblico replicato sui computer di tutti i possessori di tale valuta. La gestione di tale registro, nel momento in cui devono essere convalidate le transazioni in corso, richiede una potenza di calcolo estremamente elevata (e quindi anche un enorme dispendio di energia elettrica, ragione per cui tale tecnologia non è sostenibile dal punto di vista ambientale[29]). Per incentivare all'impegno di tale potenza di calcolo la convalida delle transazioni è accompagnata dal "conio" di nuova valuta utilizzata per remunerare l'autore della convalida. Per questo l'attività di calcolo necessaria è detta *mining*, richiamando l'idea del minatore. La criminalità informatica sfrutta questo meccanismo per arricchirsi sfruttando una tecnica detta *cryptojacking*: mediante appositi *crypto mining malware* infettano i computer di milioni di ignari utenti che vedono aumentare le proprie spese per l'energia elettrica e rallentare le loro normali attività perché i computer sono impegnati a eseguire il *mining* per conto dei criminali. Questa forma di attacco informatico è, al momento, estremamente interessante per la criminalità organizzata in quanto le crittovalute sono lo strumento tipico per transazioni illegali fornendo un buon livello di anonimato. Infatti nel 2018 il fenomeno del *cryptojacking* è cresciuto di 40 volte rispetto al 2017[30]; si aggiunga a questo il

---

(26) Si veda, per esempio, *https://www.mcafee.com/enterprise/en-us/about/newsroom/press-releases/press-release.html?news_id=20181218005639*.

(27) Recentemente alcuni governi le hanno riconosciute, mentre altri le hanno addirittura vietate.

(28) La tecnica più comune per realizzarlo si basa su strutture dati crittografate dette *blockchain*.

(29) Il consumo anno di energia per la sola valuta *Bitcoin* attualmente è stimato in circa 50 Twh (50.000.000 di MWh), equivalente al consumo anno di interi Paesi come la Grecia (*https://digiconomist.net/bitcoin-energy-consumption*).

(30) *https://www.forbes.com/sites/donnafuscaldo/2018/12/28/crypto-mining-malware-grew-4000-this-year/#8e94ec7224c2*.

fatto che le crittovalute si prestano a numerosi altri crimini informatici, quali le estorsioni basati sui *malware* di tipo *cryptolocker*[31].
L'altro settore in grande crescita per la criminalità *cyber* è quello della *Internet of Things*. Come già detto, questo nuovo scenario si basa su un gran numero di dispositivi autonomi collegati in rete[32]. Proprio il gran numero e l'autonomia rappresentano le due principali criticità dal punto di vista della sicurezza. Il primo aspetto richiede costi contenuti, che implica limitata potenza di calcolo (e quindi limitata possibilità di impiegare tecniche crittografiche "forti"), bassi costi di produzione (incluse economie nello sviluppo del *software*), ampio affidamento a soggetti terzi di attività di sviluppo e produzione (allungando la catena della fiducia). L'autonomia talvolta implica anche autonomia energetica (che quindi limita ulteriormente la potenza di calcolo per contenere i consumi), ma anche meccanismi automatici di configurazione e aggiornamento del *software*; così, se un attaccante riesce a intromettersi in tali procedure non c'è più modo di ripristinare il funzionamento corretto del sistema[33] in quanto tali automatismi escludono la possibilità di intervento diretto dell'utente[34]. Una verifica diretta di quanto i dispositivi IoT siano vulnerabili può essere effettuata semplicemente visitando *Shodan* (https://www.shodan.io/), il motore di ricerca che fornisce le informazioni necessarie per accedere ai dispositivi IoT dislocati in tutto il mondo che presentano lacune dal punto di vista della sicurezza.
La ragione per cui i dispositivi IoT sono oggetto di grande interesse per la criminalità organizzata consiste nel loro numero. Una tipologia di at-

---

(31) I *cryptolocker* sono programmi che crittografano il contenuto dei dischi e dei supporti di memoria del computer della vittima rendendoli inaccessibili e chiedendo poi un riscatto a fronte del pagamento del quale, che normalmente deve avvenire in *bitcoin*, viene rilasciata la chiave necessaria per la decrittografia.

(32) Nel 2018 il numero di dispositivi IoT nel mondo ha superato i 23 miliardi, molti studi stimano una crescita esponenziale nei prossimi anni, raggiungendo i 75 miliardi nel 2025 (si veda per esempio *https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/)*.

(33) Il problema della sicurezza della *Internet of Things* è ben illustrato dal celebre motto "*The 'S' in IoT stands for 'security'. And yes, I'm aware there's no 'S' in IoT!"*

(34) Il problema è aggravato dal fatto che proprio i dispositivi IoT più semplici non solo non dispongono di strumenti di interazione con l'utente, ma presentano anche capacità elaborative limitate che impediscono l'impiego di tecniche di protezione sofisticate.

tacco molto diffusa è il cosiddetto *Denial of Service* (DoS). Si tratta di bloccare il normale funzionamento di un sistema, di un servizio o di un collegamento di rete. Scopi degli attacchi DoS possono essere il danneggiamento di concorrenti commerciali, estorsioni ma anche preparazione di ulteriori attacchi basati su *social engineering*. Tuttavia, esistono strumenti tecnici per il controllo e il blocco del traffico di rete proveniente dai nodi sorgenti di attacchi DoS, rendendoli così inefficaci. Per questo sono state sviluppate tecniche di attacco di tipo *Distributed Denial of Service* (DDoS) che, facendo uso di un elevato numero di sorgenti coordinate, rendono molto più difficile, e talvolta impossibile, bloccare l'attacco. Queste sorgenti non sono altro che computer e altri apparati digitali violati in precedenza in cui sono stati nascosti programmi pronti per agire come sorgenti di un attacco DDoS che silenziosamente restano in attesa del relativo comando da parte del sistema di controllo centrale gestito dall'*hacker*. Reti di dispositivi violati in questo modo prendono il nome di *botnet* (cioè "rete di automi"). È evidente che il gran numero e la vulnerabilità dei dispositivi IoT rendono questi gli strumenti ideali per realizzare potenti *botnet*. Infatti, sul *black market* sono in vendita servizi per attacchi DDoS basati su *botnet* di dispositivi IoT a prezzi contenuti[35], variabili in funzione della durata e della quantità di nodi utilizzati per l'attacco. Attacchi di questo tipo sono utilizzati per bloccare reti e sistemi aziendali chiedendo un riscatto in *bitcoin*. L'elevato numero di dispositivi IoT infetti (in rapida crescita) rende queste *botnet* in grado di generare traffico di rete dell'ordine dei *terabit* al secondo (cioè migliaia di miliardi di *bit* al secondo, equivalenti a centinaia di migliaia di collegamenti ADSL residenziali). Questo ordine di grandezza del traffico di rete può bloccare non solo una singola azienda, ma un'intera nazione, spostando lo scenario dalla criminalità organizzata che agisce a scopo di lucro a organizzazioni governative (*Cyber War*) o non governative (*Cyber Terrorism*). Proprio queste considerazioni devono essere alla base della progettazione, realizzazione e gestione dei servizi della pubblica amministrazione, con tanta più attenzione quanto più essenziale o critico è il servizio.

---

(35) *https://securelist.com/the-cost-of-launching-a-ddos-attack/77784/*.

4. *Linee guida orientate alla prevenzione*

Risulta evidente quindi che il problema della *cybersecurity* coinvolge tutti i soggetti che fanno parte del moderno mondo digitale. Tutti agiscono in esso e tutti sono responsabili della sua sicurezza, seppur con ruoli differenti, in quanto comportamenti incauti o, peggio, illegali possono essere il punto di partenza di attacchi devastanti. Al di là dei dettagli tecnici è fondamentale dotarsi di linee guide orientate alla sicurezza e alla prevenzione. Il principio fondante è quello molto diffuso tra gli esperti di sicurezza e citato esplicitamente nel libro *Secure Programming Howto*[36]: "*Paranoia is a Virtue*". Nel settore della *cybersecurity* non ci si può affidare alla speranza che un evento avverso non accada in quanto gli automatismi dei sistemi di attacco rendono ogni dispositivo, sistema o servizio un bersaglio a prescindere dalla sua importanza. Diverse azioni sono già in essere per la protezione delle infrastrutture critiche e dei servizi digitali nei paesi dell'Unione europea. In Italia, su questo tema, è stata recepita nel 2018[37] la direttiva europea sulle «misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione»[38] ed è stato attivato il Dipartimento per le informazioni per la sicurezza[39]. Per le pubbliche amministrazioni l'AGID (la già citata Agenzia per l'Italia digitale) ha emanato delle circolari orientate alla prevenzione del *cyber* rischio[40]. Si tratta di un importante passo in avanti anche se principalmente orientato, per ora, ai soli aspetti tecnologici nella gestione dei sistemi. È auspicabile, per il futuro, che questa attività di prevenzione includa azioni per la diffusione della consapevolezza del problema della *social engineering* e linee guida per il progetto e la gestione di servizi basati anche su IOT. Per quanto riguarda la

---

(36) D.A. WHEELER, *Secure Programming Howto*, *https://dwheeler.com/secure-programs/*, cap. 2.6.

(37) D.lgs. 18 maggio 2018, n. 65.

(38) *https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32016L1148*.

(39) *https://www.sicurezzanazionale.gov.it/sisr.nsf/index.html*.

(40) AGID, *Misure minime di sicurezza ICT per le pubbliche amministrazioni*, *https://www.agid.gov.it/it/sicurezza/misure-minime-sicurezza-ict*, circolare 18 aprile 2017, n. 2, 2017, pubblicata in Gazzetta ufficiale della Repubblica italiana, Serie Generale n. 103, 5.5.2017, *https://www.agid.gov.it/it/sicurezza/misure-minime-sicurezza-ict*.

consapevolezza, in ambito internazionale sono in atto numerose iniziative per promuovere l'educazione alla sicurezza informatica sia dei privati cittadini che dei professionisti e dei dipendenti di enti e imprese. Per esempio, l'ENISA[41] (*European Union Agency for Network and Information Security*) ha pubblicato guide specifiche sul tema della consapevolezza[42] e sulle strategie aziendali per diffonderla e valutarla[43], mentre l'EUROPOL[44] ha redatto guide orientate alla prevenzione nei numerosi ambiti specifici della *cybersecurity*[45].

Per quanto visto finora, nella creazione, gestione e fruizione di un servizio si incontrano numerosi soggetti, ciascuno con le proprie responsabilità e il proprio ruolo. Nel caso di servizi per l'amministrazione digitale essi sono, principalmente:

- ente o struttura della pubblica amministrazione, in qualità di committente;
- i progettisti dell'architettura e gli sviluppatori dei programmi applicativi specifici del servizio;
- i fornitori dei servizi infrastrutturali (per esempio collegamenti in rete, *data center*, servizi *cloud*, ecc.);
- gli utenti.

Il committente deve essere consapevole del problema della *cybersecurity* e deve definire le specifiche del servizio valutandone adeguatamente la criticità e, in funzione di essa, rendendo disponibili adeguate risorse dedicate alla prevenzione del rischio *cyber*. Inoltre, deve essere in grado di includere clausole relative ai necessari requisiti di sicurezza nei contratti di fornitura (stipulando i cosiddetti SLA, *Service Level Agreement*).

---

(41) *https://www.enisa.europa.eu/.*

(42) *ENISA's ten security awareness good practices, European Network and Information Security Agency (ENISA)*, 2009.

(43) *The new users' guide: How to raise information security awareness*, European Network and Information Security Agency (ENISA), 2010.

(44) *https://www.europol.europa.eu/.*

(45) *https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides.*

I progettisti, gli sviluppatori e i fornitori dei servizi infrastrutturali devono adottare rigorose procedure operative atte a minimizzare le vulnerabilità dei sistemi. Poiché è pressoché inevitabile il ricorso a dispositivi e moduli *software* di provenienza esterna, è necessario valutarne ed eventualmente testarne accuratamente l'affidabilità. In generale, ma soprattutto nell'ambito dei servizi basati in toto o in parte su *Internet of Things*, che interagiscono direttamente e autonomamente con il mondo reale, i responsabili della progettazione devono essere consapevoli delle possibili vulnerabilità e operare sia per la protezione del sistema che per la garanzia di livelli minimi di servizio anche in caso di attacchi, eventualmente utilizzando strumenti alternativi.
Gli utenti finali (di ogni tipo: aziende, professionisti e privati cittadini) devono essere istruiti sul rischio *cyber* e guidati in un uso consapevole e prudente dei loro dispositivi e della rete.

5. *Conclusioni*

Tutti i servizi digitali, e quelli della amministrazione digitale in particolare, sono interessati dal problema della *cybersecurity*. Le vulnerabilità dei sistemi hanno numerose cause e il loro impatto è amplificato dal fatto che le violazioni non sono direttamente osservabili e in genere restano nascoste finché non producono danni evidenti. A tutti i livelli l'attenzione alla sicurezza deve essere parte integrante della definizione, progettazione, realizzazione e gestione dei servizi. Inoltre, come visto, la prevenzione non può essere soltanto tecnologica perché le tecnologie digitali hanno alimentato il fenomeno della *social engineering*, in cui obiettivo dell'attacco è l'essere umano che, abilmente ingannato, viene utilizzato come tramite per superare le protezioni dei sistemi informatici. Per questo, l'amministrazione digitale non deve limitare il suo ruolo a quello di erogatore di servizi, ma deve fungere anche da motore di crescita culturale del Paese. Il passaggio al digitale rappresenta l'occasione per diffondere conoscenza e consapevolezza e va assolutamente colta, a tutela dei singoli individui come dell'intera collettività.