Cybersecurity Trends

Edizione italiana, N. 3 / 2018

INTERVISTE VIP:

- Daniele GAMBETTA
- Carlo RATTI
- Roberto MASIERO

GLOBAL CYBER SECURITY CENTER

ISSN 2559 - 1797 / ISSN-L 2559 - 1797

Central Folder: Smart City

Global Cyber Security

La Fondazione GCSEC è un'organizzazione senza scopo di lucro, creata per promuovere la sicurezza informatica in Italia e nel resto del mondo. Il Centro, fondato e finanziato da Poste Italiane, ha sede a Roma e collabora con Istituzioni Italiane e Internazionali Governative, enti privati, istituti di ricerca e organismi internazionali.
La missione della Fondazione è quella di sviluppare e diffondere la conoscenza e la consapevolezza sulla sicurezza informatica, creando le condizioni per migliorare le capacità, le competenze, la cooperazione e la comunicazione tra i diversi attori coinvolti nell'uso e nella protezione di Internet.

Information Sharing
Creazione di modelli di information sharing pubblico - privato

Threat Intelligence
Analisi di modelli di attacco e delle tecnologie necessarie a velocizzare l'analisi stessa

Sensibilizzazione
Campagne di sensibilizzazione multi-livello

Formazione
Attività di formazione e corsi di specializzazione e master

Fondazione Global Cyber Security Center
Viale Europa, 175 – 00144 Roma
www.gcsec.org

GLOBAL CYBER SECURITY CENTER

Prevenire è meglio che curare

Autore: Nicola Sotira

Il 14 Agosto la pausa estiva è stata bruscamente interrotta dalla tragica notizia del crollo del ponte di Genova e delle sue vittime. Tutti coloro che vogliono un po' di statistica e analisi dei numeri possono consultare la lista, incompleta, degli incidenti che riguardano ponti a partire dal 1800 al link *https://en.wikipedia.org/wiki/List_of_bridge_failures:* pagina aggiornata con il recente evento di Genova, vedremo che questa drammatica problematica è equamente condivisa nel nostro pianeta.

Nei giorni successivi all'incidente, abbiamo appreso la storia del ponte, i giornali hanno riempito gli articoli sulle costruzioni di Morandi, retroscena, ricerche di responsabilità, ma qualcuno avrà anche notato che si è parlato di sensori e di come questi avrebbero potuto agire sulla prevenzione.

Da questa lezione tutti hanno sicuramente imparato che la salute è una questione importante non solo per gli esseri umani, ma anche per le infrastrutture del paese. Il crollo di un ponte causa vittime e conseguenze sociali ed economiche negative. Soluzioni di monitoraggio strutturale delle infrastrutture potrebbero mitigare problemi proprio nello stesso modo in cui lo screening medico di routine può scongiurare malattie.

Il monitoraggio della salute strutturale delle infrastrutture cerca di usare i sensori per rilevare danni su strutture civili, ponti e abitazioni per esempio. C'è una lunga storia di studi e ricerche su questa tematica che propone oggi anche tecnologie mature e connesse alla rete.

Ci sono sul mercato sensori che potrebbero darci molte informazioni sull'integrità strutturale o sui danni presenti su di un ponte o altra infrastruttura civile. Si va dai misuratori di forza ai sensori a fibra ottica che possono rilevare deformazione o danni nelle strutture. Inoltre, con dei sensori come gli accelerometri è possibile misurare in modo efficiente le vibrazioni dei ponti. Tutti questi dati raccolti dai sensori possono poi essere elaborati e rilevare, per esempio, cambiamenti nei modelli di vibrazione del ponte che possono indicare potenziali danni.

Il vantaggio di queste reti per il controllo strutturale è che queste sono sempre attive, ovvero consentono un monitoraggio in tempo reale, mentre oggi queste infrastrutture vengono controllate manualmente da squadre di ingegneri, con costi che impattano sulla manutenzione oltre a darci uno studio datato.

Altro tema è quello della prevenzione, l'uso di queste tecnologie ci permetterebbe di rilevare i danni molto prima, il che renderebbe non solo più sicura l'infrastruttura, ma anche molto più economica la riparazione. Ovviamente, in caso di calamità naturali, come ad esempio un terremoto, il monitoraggio dell'integrità potrebbe essere svolto in tempo reale e in caso di problematiche provvedere a segnalare la chiusura di tratti autostradali o accessi. In questo numero abbiamo deciso di parlare di Smart City, un tema che affrontiamo per capire le implicazioni e impatti relativi alla Cyber Security. Pensiamo che l'impiego di queste tecnologie, in modo sicuro, possa dare enormi vantaggi in queste aree e aumentare la sicurezza fisica che oggi più che mai è sempre più connessa al digitale. ■

Buona Lettura

BIO

Nicola Sotira è Direttore Generale della Fondazione Global Cyber Security Center GCSEC e Responsabile del CERT di Poste Italiane. Lavora nel settore della sicurezza informatica e delle reti da oltre venti anni con un'esperienza maturata in ambienti internazionali. Contesti nei quali si è occupato di crittografia e sicurezza di infrastrutture, lavorando anche in ambito mobile e reti 3G. Ha collaborato con diverse riviste nel settore informatico come giornalista contribuendo alla divulgazione di temi inerenti la sicurezza e aspetti tecnico legali. Docente dal 2005 presso il Master in Sicurezza delle reti dell'Università La Sapienza. Membro della Association for Computing Machinery (ACM) dal 2004 e promotore di innovazione tecnologica, collabora con diverse start-up in Italia e all'estero. Membro di Italia Startup nel 2014 dove con alcune società ha partecipato allo sviluppo e progetto di servizi in ambito mobile e collabora con Oracle Security Council.

Indice - Cybersecurity Trends

Indice

Foto di copertina: © Matt Milton

Sit tibi terra levis amice! Un ultimo omaggio a Romulus Maier

Autore: Laurent Chrzanovski

Romulus Maier

Il 19 luglio scorso, con la sua consueta discrezione, Romulus Maier ci ha lasciati, dopo una lunga e dolorosa malattia che ha fronteggiato con un coraggio difficile da descrivere. Altrettanto difficile è trovare le parole per rendere un omaggio a uno dei due grandi fondatori dei media IT in Romania.

È proprio con quel coraggio, con quella discrezione e con quella umiltà che erano le sue caratteristiche «genetiche», con poche parole e molti fatti che, nel 1992, decise di affrontare la difficile strada di direttore, editore e redattore di media dedicati al mondo della tecnologia, fondando il gruppo media AGORA. Per chi non conosce la storia recente del paese, e per meglio carpire la forza e l'entusiasmo necessario per iniziare allora una tale sfida, è doveroso ricordare che il 1992 fu proprio l'anno più buio dell'economia rumena, con un PIL ridotto a metà, conseguenza diretta della sfiducia degli investitori nel paese dopo l'ultima sanguinosa repressione di studenti e contestatari – nel settembre del 1991 – ad opera di gruppi di minatori chiamati a sostegno dal governo.

Quanta strada ha percorso Romulus in 26 anni di carriera! Ha dato nascita ad innumerevoli congressi annui di profilo, ed ha pubblicato molte riviste, tra le quali spiccano *«If », «PC Report», «Open – Tehnologia Informației», «Byte România», «Net Report», «Gazeta de informatică», «PC Magazine România», «eWeek România», «IT Trends»*, o ancora *«Digital Trends»*.

Dietro le quinte, come sempre, Romulus è stato il *"magnus artifex"* che ha reso possibile il lancio e la buona realizzazione delle prime edizioni del congresso annuo di dialogo mirato all'Europa Centrale *"Cybersecurity-Romania"* di Sibiu – oggi proposto anche con una variante dedicata all'Europa Occidentale, in Svizzera, ed una variante dedicata al Mediterraneo, a Noto.

Sempre in questo ambito, nel gennaio 2015, quando l'ITU e numerosi enti ci chiesero di valutare se era possibile trascrivere per i posteri i fruttuosi dibattiti di Sibiu su una rivista, incontrai Romulus in un caffè di Bucarest. Ben conscio che una tale iniziativa sarebbe stata innanzitutto un sacerdozio volontario, mi rispose flegmaticamente, *"ma sì, dai, lo facciamo: una rivista ogni tre mesi"*. Il primo volume di ***Cybersecurity Trends*** in lingua rumena fu data alle stampe due mesi dopo…

Lo stesso anno, congresso e rivista ottennero dall'ITU la massima gratificazione possibile, quella di *"Example of good practices for the European Continent"*. Oggi, la rivista trimestrale esiste in 5 lingue, grazie a partner internazionali di prestigio, tra i quali il GCSEC, che cura la versione italiana.

Lavorate da Romulus e dalla sua équipe a Bucarest, con testi di specialisti da tutta l'Europa, le versioni di ***Cybersecurity Trends*** offrono gratuitamente un po' di cultura di sicurezza da Roma a Londra, da Berlino a Parigi e, ovviamente, in Romania e Repubblica Moldova.

Il secondo volume di quest'anno è uscito pochi giorni prima che Romulus partisse verso altri orizzonti. L'abbiamo presentito amaramente perché di solito, una volta pronte, completate e corrette le edizioni, arrivava lui con mille idee, dalle più serie alle più comiche, per scegliere assieme l'immagine di copertina delle varie versioni, ad eccezione di quella italiana. Era il nostro momento di relax, di battute, di discussioni su di tutto, consapevoli che il grosso del lavoro era ormai dietro di noi. Stavolta non è stato così. Stavolta, nei nostri cuori, è Romulus che figura su ogni copertina. C'è un po' di Romulus in ogni pagina delle riviste che avete letto, leggete e leggerete in futuro. È calato il sipario, è partito un Gran Signore che ha scritto la storia dei media IT in Romania ed anche all'estero. Ora sta a noi mantenere viva la fiamma che non si sarebbe accesa senza di lui. ■

Il primo numero di Cybersecurity Trends (marzo 2015) e alcune delle riviste pubblicate da Romulus.

I rischi del life-logging

Autore: Giancarlo Butti

Gli strumenti che ogni cittadino ha oggi a disposizione e lo IOT, se da un lato introducono una serie di agevolazioni, dall'altro costituiscono una forte fonte di rischi[1] dei quali è opportuno essere consapevoli.

Il primo e più ovvio rischio in cui ogni utente incorre in una realtà sempre più interconnessa riguarda la possibilità che enti, aziende, servizi di sicurezza[2] hanno di profilare gli individui in maniera sempre più accurata attraverso l'uso dei Big Data, collezionando ed aggregando informazioni provenienti da diverse fonti quali:

- i social network;
- i sistemi di messaggistica;
- le preferenze espresse durante la navigazione su internet;
- gli elettrodomestici intelligenti;
- i contatori del consumo energetico;
- i dispositivi indossabili;
- i navigatori e geolocalizzatori o semplici smartphone[3];
- i punti di connessione wifi.

Un rischio per ogni cittadino che si estende però molto al di là della semplice sfera privata, a causa da un lato della inconsapevolezza dello stesso e dall'altra dalla mancanza di regole che stiano al passo con l'evoluzione di quanto la tecnologia offre.

Sono molteplici gli esempi di "incidenti" causati da questa persistente tracciatura:

- la localizzazione di una base militare in base ad un dispositivo indossabile con localizzatore GPS da parte di un militare durante il proprio tempo libero;
- il monitoraggio remoto delle abitazioni nelle quali siano installate telecamere che permettono tale funzionalità e per le quali non sia stata modificata la password di default o si siano utilizzate password facilmente individuabili;
- la determinazione dei periodi di presenza/assenza dalla propria abitazione in funzione dei consumi energetici;
- la pubblicazione sulle proprie pagine social dei periodi di vacanza (e quindi di mancato presidio della propria abitazione);
- la ricostruzione dei reali spostamenti di un coniuge infedele consultando le impostazioni del navigatore.

Tali incidenti, come si evince dagli esempi, possono essere causati da:

- informazioni rese disponibili volontariamente dall'utente;
- tracce lasciate involontariamente dall'utente durante lo svolgimento di un'attività, disponibili on line liberamente o "acquistate" dal soggetto che desidera utilizzarle;

BIO

Giancarlo Butti ha acquisito un master in Gestione aziendale e Sviluppo Organizzativo presso il MIP Politecnico di Milano.
Si occupa di ICT, organizzazione e normativa dai primi anni 80 ricoprendo diversi ruoli: security manager, project manager ed auditor presso gruppi bancari; consulente in ambito sicurezza e privacy presso aziende dei più diversi settori e dimensioni.
Affianca all'attività professionale quella di divulgatore, tramite articoli, libri, whitepaper, manuali tecnici, corsi, seminari, convegni. Svolge regolarmente corsi in ambito privacy, audit ICT e conformità presso ABI Formazione, CETIF, ITER, INFORMA BANCA, CONVENIA, CLUSIT, IKN, Università degli studi di Milano.
Ha all'attivo oltre 700 articoli e collaborazioni con oltre 20 testate tradizionali ed una decina on line. Ha pubblicato 21 fra libri e whitepaper alcuni dei quali utilizzati come testi universitari; ha partecipato alla redazione di 9 opere collettive nell'ambito di ABI LAB, Oracle Community for Security, Rapporto CLUSIT…
È socio e proboviro di AIEA, socio del CLUSIT e di BCI.
Partecipa ai gruppi di lavoro di ABI LAB sulla Business Continuity, Rischio Informatico e GDPR di ISACA-AIEA su Privacy EU e 263, di Oracle Community for Security su frodi, GDPR, eidas, sicurezza dei pagamenti, SOC, di UNINFO sui profili professionali privacy, di ASSOGESTIONI sul GDPR…
È membro della faculty di ABI Formazione, del Comitato degli esperti per l'innovazione di OMAT360 e fra i coordinatori di www.europrivacy.info. Ha inoltre acquisito le certificazioni/qualificazioni LA BS7799, LA ISO/IEC27001, CRISC, ISM, DPO, CBCI, AMCBI.

- informazioni ottenute violando sistemi di sicurezza inadeguati (come nel caso delle telecamere prima citate).

Le informazioni così raccolte possono essere successivamente utilizzate per valutare, da parte delle aziende o di altre organizzazioni:

- le abitudini e comportamenti degli utenti per finalità di marketing;
- l'affidabilità economica di un utente, ai fini della concessione di un prestito;
- la salute di un utente, ai fini assicurativi;
- le idee e comportamenti di un utente, ai fini di una valutazione di idoneità per una posizione lavorativa;
- la localizzazione di basi militari da parte di forze ostili.

È interessante notare come in questo ultimo caso, dalle conseguenze potenzialmente letali, gli episodi individuati e disponibili on line continuino a verificarsi, a testimonianza che anche i settori per i quali ci si aspetterebbero i più alti livelli di sicurezza e consapevolezza siano in realtà fragili e poco presidiati da questo punto di vista.

Inoltre anche i cittadini più attenti a limitare le proprie tracce e virtuosi nell'uso degli strumenti e nel concedere i propri dati, possono comunque subire delle conseguenze da questo costante monitoraggio.

I loro dati infatti sono, loro malgrado, diffusi da parte degli altri utenti della rete, o presenti sui loro dispositivi (di solito poco protetti) e quindi facilmente acquisibili da parte di terzi in caso di furto o smarrimento.

Al riguardo va precisato che, inspiegabilmente, il nuovo regolamento europeo sulla privacy limita notevolmente la tutela prevista in tal senso per i cittadini.

Il D. Lgs 196/03 infatti prevedeva forti tutele per il trattamento dei dati personali anche da parte di un semplice cittadino. In prima istanza chiunque trattasse dati personali (comprendendo con questo anche l'avere una semplice rubrica sul proprio cellulare o delle foto di altri soggetti sul proprio smartphone) era tenuto ad implementare adeguate misure di sicurezza e rispondeva civilmente in caso di danni provocati dalla propria negligenza in tal senso.

In secondo luogo era espressamente vietato pubblicare su internet, o comunque diffondere, dati di terzi senza il loro specifico consenso.

Ora la formulazione presente nel GDPR è molto ambigua, in quanto le tutele da esso previste non si applicano quando i trattamenti sono:

"c) effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico

definendo queste ultime come:

Le attività a carattere personale o domestico potrebbero comprendere la corrispondenza e gli indirizzari, o l'uso dei social network e attività online intraprese nel quadro di tali attività."

Su tale definizione si discute in merito al fatto che il perimetro di non tutela riguardi esclusivamente una pubblicazione di dati nell'ambito della propria cerchia di contatti o se effettivamente sia concessa una assoluta libertà di pubblicazione di dati di terzi, la cui tutela è affidata quindi ad altre normative molto più onerose da invocare.

In ogni caso il "rafforzamento" della tutela degli interessati, con cui viene da sempre presentato il GDPR ha su questo aspetto, almeno nei confronti della normativa italiana, un vistoso punto di debolezza.

I comportamenti e l'inconsapevolezza o più semplicemente la superficialità con cui un soggetto lascia le proprie tracce informatiche hanno effetti quindi non solo su di lui, ma anche su soggetti terzi ed in altri ambiti, ad esempio mediante la pubblicazione sui social di informazioni in merito alla propria attività lavorativa con la rilevazione involontaria di informazioni che l'azienda considera riservate (progetti sui quali si è o si sta lavorando, nuove sedi...).

È evidente che in questo caso una grossa parte di responsabilità va fatta ricadere sulle aziende, che non regolamentano e non istruiscono adeguatamente i propri dipendenti in merito alle conseguenze di determinati comportamenti, non provvedono ad emanare specifiche social policy che regolino la materia e non danno una chiara indicazione di quali siano le informazioni che debbano considerarsi riservate.

paal
Privacy-Aware and Acceptable Lifelogging services for older and frail people

Dal punto di vista della relazione fra utente ed azienda giova anche ricordare che è lecito per un'azienda utilizzare il materiale pubblicato sui social dai propri dipendenti per fini disciplinari, laddove tale materiale violi i principi di fedeltà.

Un altro aspetto che si tende a sottovalutare è la persistenza delle tracce informatiche delle proprie azioni, che persistono per anni sia nella loro forma originale, sia sotto forma di successive rielaborazioni ed aggregazioni e sfuggono completamente al controllo dell'utente. Il diritto all'oblio, previsto dal GDPR, copre solo in minima parte questo aspetto, in quanto presuppone una corretta, puntuale e trasparente gestione dei propri dati personali da parte dei vari titolari di trattamento, ma la realtà è ben diversa.

Il titolare che ha reso disponibile il dato potrebbe anche in teoria eliminarlo dalla rete, ma non è possibile intervenire su tutti i soggetti che il dato hanno visionato o scaricato, o aggregato ad altri dati che riguardano l'utente.

Per non parlare delle repliche o delle copie che vengono effettuate per motivi di sicurezza e continuità operativa, o sulle quali ben difficilmente, al di là della teoria e delle imposizioni della normativa, sarà possibile intervenire.

Nella realtà dei fatti quindi ciò che viene messo in rete volontariamente dagli utenti, o le informazioni raccolte sul loro comportamento derivante da loro azioni (ad esempio la navigazione su un sito) o da dispositivi in dotazione, ha una persistenza estremamente più lunga di quello dallo stesso desiderato.

L'unica possibilità di difesa è quindi acquisire una maggior consapevolezza nel rilasciare le proprie informazioni e nell'impostare correttamente, almeno dove possibile, gli strumenti che si hanno a disposizione. ■

1 *To Log or not to log?* Enisa 2011

2 *Intelligenza artificiale e soft computing nella lotta al terrorismo*, G.Butti, www.sicurezzanazionale.gov.it

3 Grazie a Pin Me è possibile localizzare la posizione di uno smartphone: *Pin Me: Tracking a Smartphone User around the World,* Mosenia-Dai-Mittal-Jha

Smart City: un futuro luminoso o un'oscura minaccia?

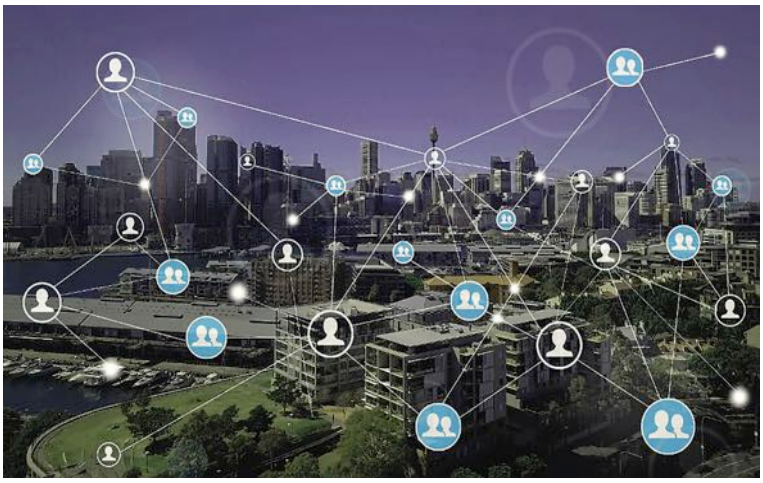
Autore: Viviana Rosa

Entro il 2050, si stima che il 70% della popolazione mondiale vivrà nelle città. Attualmente, in Italia, già oltre il 70% della popolazione è urbana. Pertanto, è fondamentale garantire già da oggi che le città forniscano un ambiente sicuro e piacevole in cui vivere e lavorare, in modo sostenibile e resiliente ai cambiamenti. Questo deve essere l'obiettivo di una "Smart City". La PAS 180 di BSI descrive la Smart City come "una realtà che integra efficacemente i sistemi fisici, digitali e umani in un ambiente costruito per offrire un futuro sostenibile, prospero e inclusivo per tutti i suoi cittadini ".

Le tecnologie digitali e i dati associati rappresentano un'enorme opportunità per migliorare le esperienze e la qualità della vita in tutti gli aspetti della società, dalla casa al posto di lavoro, ai trasporti, ai servizi pubblici, alla salute, allo svago, all'agricoltura, allo shopping e alla distribuzione.

BIO

Viviana Rosa ricopre il ruolo di Commercial Director in BSI Group Italia, azienda nella quale entra nel 2010, e per la quali si occupa della strategia commerciale e marketing oltre che dell'introduzione di nuovi prodotti nel settore della Sicurezza e del Risk Management.
Durante la sua carriera professionale, per diversi anni, ha ricoperto ruoli di rilevanza internazionale seguendo importanti progetti di comunicazione, marketing e vendite per realtà di svariati settori, instaurando solidi rapporti con gli stakeholder di riferimento, comprese le amministrazioni pubbliche e gli enti governativi.
Laureata in Lingue e Letterature Straniere presso l'Università Cà Foscari di Venezia ha ottenuto una specializzazione post laurea in Multimedia Content Design presso la Facoltà di Ingegneria di Firenze e ha studiato Foundation of Management a Londra presso l'ILM - Istituto di Leadership Management.

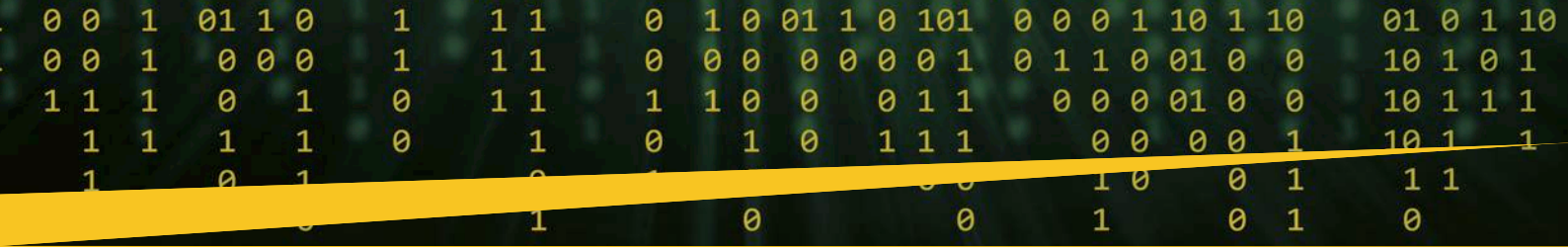


L'ascesa dell'Internet of Things (IoT), in cui sempre più dispositivi sono interconnessi per scambiarsi dati e interagire con il minimo intervento umano, unita a un'intensiva analisi del software e a una connettività estesa, ci consente di monitorare e controllare i sistemi complessi presenti in una città a un livello senza precedenti, attraverso l'inclusione di sensori e attuatori collegati. In Italia, il mercato dell'IoT è stato pari a 3,7 miliardi di euro l'anno scorso, con un aumento del 30% rispetto al 2016. Tuttavia, tutta questa connettività ha un prezzo: la sicurezza delle informazioni.

Quali sono le sfide delle città intelligenti per la cyber security?

Aumento della superficie di attacco

L'enorme crescita dei dispositivi connessi all'interno di una Smart City comporta un aumento delle possibilità di accesso per un potenziale



attaccante. In assenza di chiare indicazioni, standard e normative, i device connessi spesso non dispongono delle misure di sicurezza di base e consentono agli attaccanti di accedere facilmente ai sistemi, a potenziali fonti da dirottare *(hijacking)* per attacchi *Denial of Service* (DoS) e a obiettivi critici vulnerabili nell'infrastruttura stessa della città.

Mancanza di competenze

Esiste una carenza a livello mondiale di competenze specializzate in sicurezza delle informazioni, che si accentua nelle smart city in cui i governi locali/comuni lottano per attirare persone idonee in numero sufficiente a fornire loro una sicurezza efficace.

Diverse motivazioni di attacco

La città intelligente è soggetta a una vasta gamma di potenziali minacce, da attività criminali come *ransomware*, agli *hacktivisti* mossi da motivazioni politiche fino ad atti di terrorismo. Abbiamo visto a livello globale segnalazioni di violazioni della sicurezza, richieste di riscatto, perdite di dati personali, attacchi di tipo *Denial of Service* nei dipartimenti e nei sistemi governativi e municipali e anche attacchi a servizi pubblici e infrastrutture critiche che rappresentano una vera minaccia alla sicurezza delle persone.

Man mano che le città intelligenti si evolvono e crescono, le questioni di cui sopra diventeranno più urgenti.

Questa minaccia è reale?

Assolutamente sì! Nell'ultimo anno sono stati segnalati attacchi informatici sulle infrastrutture delle Smart City negli Stati Uniti ad Atlanta, Baltimora, San Francisco, Charlotte e Dallas. Spesso l'attacco avviene attraverso *ransomware* e con una serie di potenziali impatti che vanno dal compromettere i dati, al Denial of Service, fino a interruzioni del servizio potenzialmente pericolose per le vite dei cittadini. In realtà i servizi più critici sono stati in grado di ripristinare un sistema alternativo (di solito manuale) di riserva. Tuttavia, la quantità e la gravità di questi attacchi sta aumentando, rendendo sempre più probabile un attacco potenzialmente mortale. I vettori di attacco più diffusi e gravi sono attraverso "Advanced Persistent Threats" (minacce avanzate persistenti) in cui gli hacker mirano ad accedere alle reti in modo nascosto e riescono a rimanere inosservati per lunghi periodi fino a raggiungere i loro obiettivi.

Cosa si può fare?

Questo è un argomento molto complesso. Tuttavia, di seguito sono riportate alcune semplici linee guida per evitare le insidie più comuni.

Strategia e resilienza

Prima di arrivare alle misure di sicurezza, questo non è solo un problema tecnico da risolvere per i team ICT. Coinvolge tutte le persone e tutti i sistemi che utilizziamo nel corso delle nostre vite. Il modo più semplice per ridurre le minacce alla sicurezza non è adottare una nuova tecnologia, perché si perderebbe un'enorme opportunità. Sebbene non esista un'unica soluzione per rendere "sicura" una città, ci sono molte cose che possono essere fatte per consentire alle città e alle comunità di ottenere i benefici dalla tecnologia digitale connessa, riducendo al minimo i rischi. Questo dovrebbe far parte della strategia di resilienza di qualsiasi organizzazione. L'equilibrio tra essere difensivi (fermare le cose brutte che accadono) ed essere progressisti (facendo accadere cose buone) deve essere attentamente valutato.

Pensa in grande ma inizia in piccolo

Dove questa nuova tecnologia darà davvero un valore aggiunto? Concentrarsi inizialmente su queste aree, pensando in grande ma iniziando in piccolo, in modo controllato. Questo dovrebbe essere pensato nella strategia della città prima di impegnarsi con la tecnologia di una smart city.

Ottieni l'aiuto dagli esperti

Questo non è qualcosa che i comuni dovrebbero gestire da soli. La tecnologia, le minacce e gli scenari cambiano così velocemente che sono necessari veri esperti in materia per tenere il passo con le minacce.

Implementare una politica di sicurezza informatica end-to-end

Tendiamo a pensare alla sicurezza informatica in termini di controllo degli accessi alle nostre reti. Le principali vulnerabilità sono a entrambe le estremità del sistema. Che tu gestisca una città, una comunità, un'azienda o un'organizzazione, le regole di base sono le stesse. La sicurezza informatica inizia con i dati. La maggior parte degli attacchi continua ad entrare attraverso il *phishing*, la *social engineering* e simili. All'altra estremità del sistema ci sono i molti dispositivi IoT collegati in rete, spesso con pochissima sicurezza e con poca conoscenza o controllo a livello di sistema fornendo una superficie di attacco ampia e vulnerabile. Assicurati che la tua politica di Information Security sia completa, e che copra tutti i rischi. Come farlo in un ambiente in continua evoluzione? Lavora con esperti fidati.

Pensa alla sicurezza per tutto il ciclo di vita di un progetto

La sicurezza non è facile e non è un singolo passo nel processo. È fondamentale per la progettazione, la messa in servizio, l'uso, la manutenzione e la disattivazione del progetto. Se pianificato ed eseguito efficacemente durante la vita di un progetto, può essere la base per una "città intelligente" di successo, in cui i benefici della tecnologia intelligente possono essere realizzati da tutta la comunità. ■

Nuovi scenari digitali: occhio alla datacrazia

Intervista VIP a Daniele Gambetta

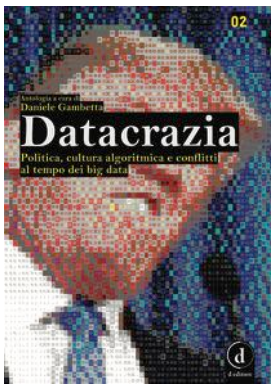
Autore: Massimiliano Cannata

Daniele Gambetta

"Parlare di dati e algoritmi vuol dire occuparsi praticamente di tutto. Delimitare il campo di indagine è già un'impresa quando si parla, infatti, di un tema complesso come la rivoluzione digitale". La prefazione del saggio *Datacrazia*, antologia curata da Daniele Gambetta (D Editore), giornalista freelance, collaboratore di numerose riviste, esperto di scienza e tecnologia, fa da incipit a quello che si può definire come un esperimento di "auto-formazione" e "co-ricerca". Abbiamo chiesto all'autore di soffermarsi sulle finalità di un'operazione editoriale che raccoglie una pluralità di validi e interessanti contributi e che presenta le sembianze di un progetto oltre che, per dirla con Umberto Eco, di "un'opera aperta".

Dottor Gambetta, ci può dire come nasce questo lavoro?

L'idea è nata un anno fa, quando con la casa editrice, D Editore, abbiamo ritenuto che i tempi fossero maturi per proporre una riflessione, soprattutto nel dibattito italiano, su aspetti politici ed economici legati allo sviluppo della società dei dati. L'influenza delle tecnologie dell'informazione è ormai pervasiva, quindi parlare di dati e algoritmi significa, come lei ricordava prima, parlare di una miriade di micro e macro processi emergenti afferenti a vari campi della produzione e del sapere. In questo contesto, la maniera più consona di procedere ci è sembrata quella di un lavoro antologico e quindi a più voci, chiedendo ad autori e autrici afferenti a diversi background (giornalisti, ricercatori, economisti, musicisti, studiosi dell'arte, attivisti…) di fornire un punto di vista specialistico in relazione ai campi di interesse, con la finalità di tessere un filo rosso, un punto interpretativo convergente.



"Datacrazia" è il titolo forte che riassume le tante questioni trattate (non-neutralità dell'algoritmo, proprietà dei dati e delle piattaforme) e che allude a una forma di potere fondato sulla conoscenza e il controllo delle informazioni. Non si era mai verificato nella storia che l'umanità potesse disporre di un giacimento talmente ricco da superare ogni immaginazione. Quali conseguenze genera un fenomeno di tali proporzioni, che vede i colossi della Rete pronti a trarre i maggiori vantaggi dallo sviluppo dei* Big Data*?

Il titolo dell'opera è tratto da una celebre citazione del sociologo Derrick de Kerckhove *("Benvenuti nella datacrazia")* ed è una chiara provocazione. Se da un lato è vero che ci troviamo di fronte a una crescita storica ed esponenziale delle tecnologie di cattura e analisi dell'informazione, dall'altro dobbiamo anche distinguere cosa è nuovo da cosa è vecchio. La propaganda è "sempre" esistita, l'analisi del target anche; oggi accade che questi processi assumono strategie complesse e in continua evoluzione, ma davanti a un non-troppo-scandalo come Cambridge Analytica dovremmo anche collocare il timore verso la tecnologia in un contesto più ampio, che riguarda anche il potere delle piattaforme, ma più in generale potremmo dire di alcuni soggetti privati che condizionano i processi democratici.

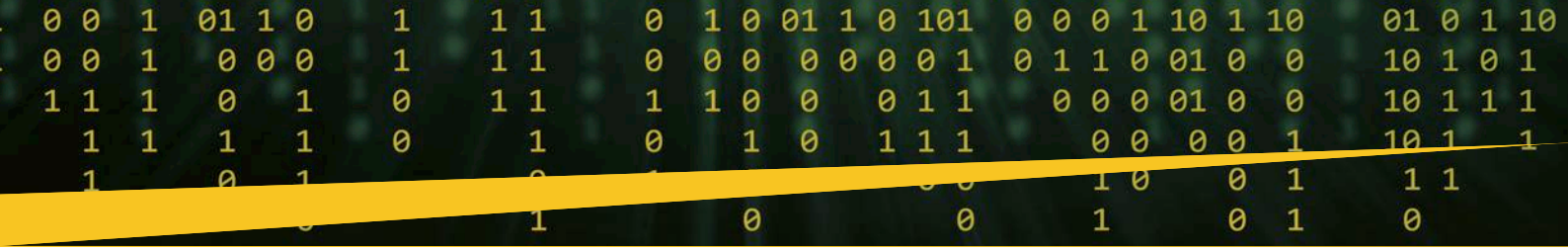
"Il mito del calcolo"

Un algoritmo oggi è in grado di valutare gli insegnanti, gli investimenti in borsa, se e quando ci ammaleremo, quale profilo assumere o licenziare, condizionando il corso delle nostre vite. Tutto appare misurabile, nella visione di una pericolosa utopia che sta espropriando l'individuo dei poteri di scelta e di decisione, che non appaiono più frutto di valutazioni culturali, maturate con l'esercizio dello studio e della riflessione umana. Quali sono i rischi di un percorso evolutivo ancora poco conosciuto e dibattuto?

Il rischio è soprattutto di carattere culturale. Uno dei temi affrontati nell'antologia è il mito della neutralità algoritmica. Chiariamo subito una cosa: non siamo luddisti o tecnofobici. Un utilizzo dell'analisi dati e degli algoritmi – ad es. del *machine learning* – può essere utile, bisogna sempre considerare però che l'output non è oggettivo e neutrale, ma frutto delle scelte

BIO

Laureato in matematica, giornalista freelance, Daniele Gambetta ha collaborato negli ultimi anni con varie riviste e testate giornalistiche - tra cui *il Manifesto, Motherboard, Fanpage, Pagina 99* - con articoli e approfondimenti di scienza e tecnologia. *Datacrazia* è la sua prima pubblicazione saggistica. Partecipa al gruppo di ricerca indipendente *HackMedia*.



e dei modelli che risiedono a monte nella fase di progettazione. Sono noti casi di algoritmi affetti da bias razzisti e sessisti, provenienti dai dataset utilizzati in fase di addestramento e di sperimentazione. Qualora un software viene utilizzato in ambito sociale è importante ricordare che esistono e hanno il loro peso le scelte politiche nella stessa progettazione di un algoritmo.

Un aspetto importante che il testo affronta riguarda la dicotomia stato/piattaforme. Stiamo assistendo a un indebolimento della sovranità nazionale insieme a uno svuotamento dei parlamenti (il dibattito sulla democrazia diretta sollevato da Grillo e Casaleggio è molto indicativo al riguardo) che appaiono non più sorretti da istituzioni forti e soprattutto credibili. La diffusione dei partiti-piattaforma, pensiamo all'esperienza italiana del M5S inizialmente sottovalutata da molti, sta cambiando le regole della partecipazione democratica? Detto in sintesi: la digitalizzazione di tutti i processi sociali è destinata a trasformare il profilo, i soggetti e i linguaggi della politica?

Credo sia troppo forte proclamare la fine degli stati, e il tema è tanto complesso quanto in divenire. Quello che è certo è che il dibattito pubblico, sulla privacy così come sulla neutralità della rete o sul copyright, il più delle volte è in ostaggio di un bipolarismo di interpretazioni sul modo di concepire il mercato dell'informazione, e in questo scontro tra titani le istanze dei lavoratori dell'informazione, il ruolo dei *prosumer* (produttore e consumatori, come gli utenti facebook), e i diritti sociali non prendono mai parte del dibattito.

Il plusvalore della Rete

Nell'economia delle relazioni il plusvalore è legato alla messa in Rete di intelligenze, idee, conoscenze. Sta però accadendo che la profilazione di utenti, il monitoraggio costante delle nostre vite generano una diffusione sistematica e un'intensificazione della precarietà. Per quali ragioni il "capitalismo delle piattaforme" ha interesse a non riconoscere la "moltitudine produttiva", che dovrebbe vedere tutti gli utenti come autori, produttori e protagonisti del business?

Il concetto di plusvalore di rete è estremamente utile per analizzare la fase attuale. Esiste continuamente un'estrazione di valore dalle nostre interconnessioni, la nostra produzione materiale e immateriale che ha luogo nelle relazioni (e qui si potrebbe anche connettere il tema alla questione del lavoro domestico e di cura), e in questo contesto le piattaforme (non solo i *social network* ma anche, ad esempio i processi di *sharing* a vari livelli) giocano chiaramente un ruolo dominante. È allora fondamentale mettere anche questo dato al centro del dibattito sul reddito di base incondizionato, che può configurarsi come una forma di riconoscimento della produzione diffusa.

Veniamo alla sicurezza, che è uno dei grandi temi del nostro tempo. Nella società digitale fondata su una stretta correlazione tra mente-macchina quali investimenti occorre fare per aumentare la tutela di quello che Rodotà definiva "il corpo elettronico"?

La privacy e la sicurezza sono oggi terreni di scontro, anche tra quei colossi di cui si parlava prima. La cessione delle nostre informazioni diventa forma di pagamento ("se non paghi, il prodotto sei tu"), o garanzia di sicurezza ("non aver nulla da nascondere"). Credo che occorra ripensare la costruzione dei rapporti sociali, oltre l'individualismo e la coercizione, è venuto il momento di immaginare istituzioni e piattaforme nuove e di rimettere al centro i diritti delle persone prima delle richieste delle multinazionali.

Proviamo a rimanere sulla trattazione dei diversi profili della sicurezza. Nello scorso mese di maggio è entrato in vigore il regolamento europeo della privacy. Cosa è cambiato in concreto per istituzioni, imprese e cittadini? Quali iniziative andranno adottate per rafforzare la cyber security?

Il nuovo regolamento della protezione dei dati (GDPR) è un insieme di linee guida, la cui applicazione poi non è sempre immediata. Per fare un esempio, nel regolamento si parla di "right to explanation", diritto alla comprensione dell'algoritmo. In primo luogo questo significa prendere una forte posizione politica nei confronti di piattaforme private, spesso chiuse e non *open source*. Inoltre spesso questa *"explanation"* è messa a dura prova dalla costruzione stessa degli algoritmi. È il caso del problema *black box* nel *deep learning*, ovvero la difficoltà, anche da parte dei ricercatori, di comprendere i meccanismi di ragionamento del software. Questo per dire che può sembrare anche fin troppo semplice delineare indicazioni su questi temi, poi la realtà è piena di aspetti complessi che vanno affrontati e risolti.

La necessità di sviluppare una cultura dell'algoritmo

Il libro parla di "cultura algoritmica". Cosa occorre fare per facilitare la diffusione di una cultura digitale nel nostro Paese?

Occorre aprire spazi di discussione, e già stanno nascendo interessanti progetti. Un concetto interessante, ripreso anche dagli attivisti del progetto europeo Decode è quello di *data commons*, ovvero la possibilità di riappropriarsi del valore prodotto dai nostri dati, in modo aggregato e/o anonimizzato, tale da poter fornire utili strumenti a una collettività nella gestione dei servizi (urbani, informativi, decisionali…).

Abbiamo nello scorso numero intervistato Michele Mezza che ha appena pubblicato il saggio "Algoritmi e libertà". Sintetizzo la sua proposta: "mettiamo gli algoritmi sul tavolo per svelare le finalità e i principi che orientano la ricerca in campi delicati come la sanità, la genetica, l'informazione in modo da far diventare la* potenza del calcolo *uno* spazio pubblico, un bene comune." *Il* Futuro possibile *auspicato in conclusione del saggio da Lei curato ha dei punti di contatto con questa posizione che tende a invocare maggiore trasparenza da parte dei grandi* player *che operano nel mercato globale?

Sicuramente sì. Ricordiamoci che quando parliamo di "svelare gli algoritmi" stiamo chiedendo sia un lavoro di sviluppo tecnico (come per la questione della *black box* del *deep learning*), ma anche e soprattutto stiamo assumendo una posizione politica, rispetto alla *closeness* (il termine vuol dire che non consentono l'accesso e la consultazione del codice, non *open source* n.d.r.) delle piattaforme proprietarie. Se la via per imporre però condizioni alle grosse piattaforme appare oggi tortuosa (chi decide su piattaforme globali?), si apre la possibilità di creazione di nuove piattaforme, radicate sui territori e le reti sociali che ne fanno uso, che possano stabilirne "le finalità e i principi che le orientano".

Quando Lei parla della necessità di* schierare strategicamente le tecnologie esistenti *per* riprogettare il mondo *intende sollecitare la politica a creare i presupposti per cambiare il corso delle cose e renderlo più vicino alle legittime aspettative di felicità e progresso dell'umanità?

Il soggetto a cui, in *Datacrazia*, rivolgiamo questa proposta, è in realtà ampio e aperto. C'è la comunità accademica, che potrebbe svolgere un ruolo chiave nella costruzione di una voce nuova nel dibattito sui dati e le regolamentazioni, ma esistono anche laboratori indipendenti, hacklab, spazi sociali e riviste culturali che ogni giorno costruiscono pratiche e analisi e quindi possibilità di aggregazione tra programmatori, comunicatori, precari e sfruttati dell'economia delle piattaforme. Da queste realtà, oggi, più che dalla politica istituzionale, mi aspetto una risposta strategica allo stato delle cose attuali. ■

Sicurezza e sviluppo umano nella città del futuro

Intervista VIP a Carlo Ratti

Autore: Massimiliano Cannata

Carlo Ratti

Professor Ratti, volendo guardare all'orizzonte della città del futuro, partirei dal tema forse più controverso e dibattuto di questo momento: la sicurezza che divide non solo gli studiosi, ma anche la politica. In contesti abitativi dominati da Reti, sensori, IOT, quali scenari si aprono sul fronte della privacy e della possibile sottrazioni di dati sensibili?

Si stanno aprendo su questo fronte scenari potenzialmente inquietanti, se non gestiti in modo appropriato. Mi viene in mente il Calvino della "Memoria del Mondo", e quel racconto di una società distopica che, per molti versi, ha punti di contatto con il nostro presente. Di fatto abbiamo già perso la nostra privacy, anche se non ce ne siamo accorti – e si tratta di un'osservazione che tocca tutti gli aspetti delle nostre vite, non solo le città. Dobbiamo ora evitare che la situazione degeneri: penso in particolare alla enorme asimmetria che esiste - quando si parla di accesso e possesso dei dati - tra pochi giganti informatici e tutti gli altri attori sociali. Per fortuna negli ultimi anni, soprattutto in Europa, è emersa una maggiore sensibilità rispetto a questi temi. Pensiamo al recente provvedimento *GDPR-General Data Protection Regulation*, che potrebbe cambiare le regole del gioco mondiali.

Gli architetti possono svolgere un ruolo nella* governance *strategica del rischio informatico, aspetto sempre più al centro dell'attenzione se si guarda alla dimensione di una paura collettiva crescente rispetto a fenomeni come il terrorismo internazionale che stanno di fatto modificando non solo il paesaggio urbano, ma anche le abitudini e gli stili di vita?

Credo che possano e debbano farlo, portando con sé quel bagaglio non soltanto tecnico ma anche umanistico che è proprio del nostro mestiere. Se non riusciranno in questo intento, verranno rimpiazzati da altre figure che presentano un taglio più squisitamente tecnico/burocratico: e questo, al di là di ogni interesse corporativo, credo sarebbe una perdita per tutti.

"La città rimane comunque un'onda in movimento", ***mi rifaccio a una celebre definizione del sociologo Franco Ferrarotti. Probabilmente la città ritratta, quella raccontata da studiosi come Franco Purini, che si rifà a un modello rinascimentale non esiste più. Nella prima parte del saggio viene utilizzata una definizione complessa:* Futurecraft*, una sorta di tavolozza proiettata su un futuro che ci riguarda. La domanda è: come, e dove vivremo domani?***

Non volendo predire il domani, evito di rispondere alla domanda! Mi limito a un commento: sono convinto che la "forma urbis" di cui mi chiedeva prima non sarà sottoposta a stravolgimenti eccessivi. I "Fundamentals" descritti da Rem Koolhaas alla Biennale di Venezia del 2014 sono destinati a restare tali, se non altro per limiti fisici e funzionali insormontabili. A cambiare insomma non sarà tanto l'aspetto, quanto le modalità di relazione all'interno dello spazio: come ci spostiamo, ci incontriamo, discutiamo, lavoriamo, o facciamo acquisti. *Futurecraft* vuol dire tracciare un processo collaborativo di definizione del domani. Un domani non da predire, ma da costruire insieme.

Un aspetto particolarmente interessante riguarda la definizione di* wiki city, (di cui si parla nella prima parte del saggio) *studiata nel duplice paradigma urbano:* top-down / botton-up, *tali modelli dovrebbero tendere a un'integrazione. A suo

BIO

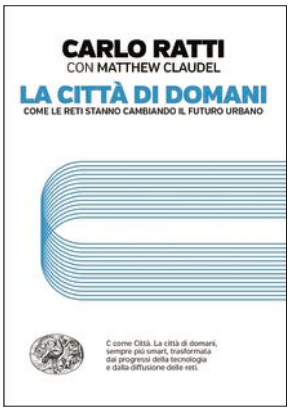
Carlo Ratti, ingegnere architetto, è docente al Massachusetts Institute of Technology, dove ha fondato il Senseable City Lab. È inoltre direttore dello studio internazionale di Progettazione "Carlo Ratti Associati" la cui sede italiana sorge a Torino. Nella "Città di Domani", saggio scritto con Matthew Claudel, ricercatore presso il Senseable City Lab, lo studioso affronta il delicato incrocio che lega sviluppo tecnologico, progettazione e visione del futuro. Al centro dell'analisi l'evoluzione dei contesti urbani attraversati dalle reti, che vivono una trasformazione profonda che prelude a nuovi equilibri ancora per molti aspetti difficili da comprendere. Hackerare la città è l'invito provocatorio all'azione e alla discussione collettiva di un architetto, tecnologo e pensatore di straordinaria vivacità, capace di saltellare da un capo all'altro del globo per affrontare i temi dell'innovazione sociale a tutto tondo.

avviso, in una dimensione urbana in divenire come quella che viviamo, ci potrà essere spazio per una cittadinanza attiva?

Mi auguro di sì. Le reti ci offrono molte nuove opportunità, ma sta a noi coglierle.

In altri termini è possibile mettere al centro dell'innovazione tecnologica il cittadino che, come si sta vedendo nei più diversi contesti, appare sempre più escluso dai processi di decisione politica?

Credo che sia fondamentale: la "smart city" non si costruisce solo dall'alto. Intendiamoci, il pubblico ha di certo un ruolo da giocare. Ad esempio il sostegno alla ricerca accademica, o l'intervento in ambiti che possono apparire meno "attraenti" al capitale di rischio – come lo smaltimento dei rifiuti o la gestione delle acque. In generale però credo che i governi dovrebbero soprattutto impiegare i loro fondi per promuovere una cittadinanza attiva e per sviluppare un ecosistema di innovazione organica rivolto alla città, simile a quello che sta crescendo naturalmente in Silicon Valley. Si tratta, come si vede, più di un approccio da basso che di schemi dall'alto verso il basso.



Le tecnologie come fattore abilitante

Un altro aspetto molto dibattuto riguarda l'utilizzazione delle tecnologie come fattore abilitante, decisivo per ridurre la polarizzazione della società, attenuare il divario tra ricchi e poveri e per superare il classico scarto tra centro e periferia. A che punto siamo su questo delicato aspetto?

Anche in questo caso si tratta di sfide aperte, che possono prendere una piega o l'altra a seconda delle scelte che riusciremo a compiere. Sono personalmente ottimista, anche se credo che una regolamentazione sia necessaria. Pensiamo all'impatto dell'intelligenza artificiale e dei processi di automazione sul mondo del lavoro. Un famoso studio dell'università di Oxford ha stimato che quasi la metà dei lavori oggi esistenti saranno resi obsoleti nei prossimi decenni. La risposta sta probabilmente nell'educazione, e in altre due parole chiave: transizione e redistribuzione.

La città è sempre stato il luogo di elezione di architetti, sociologi, urbanisti, oggi i grandi contesti sono sempre più popolati da giganti dell'informatica. Quali sono le conseguenze di questo mutamento destinato non solo ad incidere sul paesaggio urbano e antropologico, ma anche più in generale sugli equilibri di potere?

Non credo che i giganti dell'informatica – almeno per ora – costituiscano una minaccia per le città. Noto invece qualcosa di molto positivo: un approccio sempre più "anti disciplinare". Partiamo dalle università. Qualche decennio fa, le questioni digitali erano appannaggio dei soli dipartimenti di informatica e quelle urbane delle scuole di architettura. Poi, gradualmente, abbiamo assistito a una ibridazione che ha chiamato in causa altri professionisti. Il risultato è quell'approccio "anti disciplinare" che ci è molto caro, e per il quale oggi, nel nostro laboratorio di ricerca al MIT convivono architetti e informatici, fisici e sociologi, matematici e designer.

Tra futuristi e gondolieri

Sanità, traffico, reti mobili, personal communication sono tutti ambiti strategici di manifestazione dell'innovazione. Occorreranno professionalità multidisciplinari insieme a una grande capacità di visione per gestire l'elevato grado di complessità che caratterizza la rete dei sistemi ad ogni livello. Lei si muove da una parte all'altra dell'Oceano, l'Italia sul terreno della qualità professionale, delle competenze e della competitività in che posizione si colloca?

Credo che l'Italia sia un Paese che – come ha scritto il mio amico Giuliano da Empoli – si divide tra "futuristi e gondolieri": tra chi vorrebbe buttar via tutto per lanciarsi nel domani e chi invece si aggrappa al passato. Per innovare veramente invece è necessario partire dal presente e migliorarlo. Si tratta di quell'atteggiamento già delineato da Italo Calvino. Torno a citare il grande scrittore ricordando un passaggio finale delle "Città Invisibili": un modo di procedere "rischioso esige attenzione e apprendimento continui: cercare e saper riconoscere chi e cosa, in mezzo all'inferno, non è inferno, e farlo durare, e dargli spazio." In modo più specifico, se parliamo di qualità professionale, la situazione nelle nostre Università è un po' a macchia di leopardo e cambia molto anche solo da un dipartimento all'altro. Detto questo, mi sembra che i Politecnici di Torino e Milano mantengano sempre un alto profilo: è da lì che provengono molte delle persone che lavorano con noi a Torino, Boston e Singapore. Ma per fortuna si trovano eccellenze un po' ovunque nel Paese.

La riemersione di uno spazio pubblico partecipato

Per* Senseable city *cosa si intende? Si tratta di uno stadio di superamento delle Smart city, definizione che comincia ad essere criticata da molti studiosi?

Non mi piace il nome Smart City per le sue assonanze tecnocratiche, a cui non mi sento vicino. *Senseable city* è una città capace di innovare, ma anche sensibile, con la sua vocazione a integrare aspetti umanistici nella dinamica di sviluppo digitale della città. Quando abbiamo aperto il nostro laboratorio presso il MIT, nel 2004 erano ancora in pochi a parlare di Smart City: non esisteva l'iPhone, e a malapena si sapeva cosa fosse Facebook. Non saprei quindi se si tratta di un superamento: però mi fa piacere che gli aspetti per i quali si criticano le città intelligenti oggi sono quelli che avevamo già individuato quindici anni fa.

Credevamo, sulla scorta dell'insegnamento di antropologi come Marc Augé, che l'unica realtà era quella dei "non-luoghi". Invece Lei ci ricorda che i bit non hanno cancellato la distanza e hanno ridato significato ai luoghi. È in questa riemersione di uno spazio pubblico partecipato, segnato non dall'omologazione ma dalla differenza antropologica e urbana che si può realizzare il "diritto alla città" auspicato da* Henri Lefebvre*?

È vero, negli anni Novanta si credeva anche che Internet avrebbe cancellato lo spazio fisico. Non è stato affatto così. Il diritto alla città così come proposto da Lefebvre è una chiara ispirazione, ma sarebbe semplicistico negare che come progettisti agiamo in un contesto socio-economico del tutto diverso e molto più complesso rispetto ad allora.

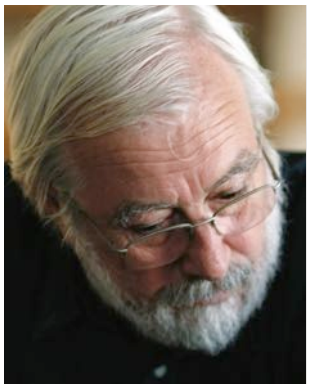
Hackerare la città, il saggio si conclude così. È un auspicio, una provocazione, la ricerca di un nuovo soggetto politico che possa aiutarci a diventare autentici "costruttori di futuro"?

È un invito all'azione e alla discussione collettiva: in linea con il principio di *Futurecraft* di cui abbiamo parlato all'inizio! ■

Smart è una modalità dell'essere, non una tecnologia

Intervista VIP a Roberto Masiero

Autore: **Massimiliano Cannata**



Roberto Masiero

"Nel digitale tutto è interconnesso, tutto è una piattaforma di relazione con le proprie singolarità e specificità, con la propria narrazione e con il modo in cui viene interpretata e, nel contempo, è inevitabilmente globale. Ciò che esiste nel digitale è nel contempo singolare e universale, locale e globale". Roberto Masiero, professore ordinario di Storia dell'architettura presso lo IUAV di Venezia, in numerosi saggi si è occupato del delicato passaggio che stiamo vivendo dall'analogico al digitale. "Niente sarà più come prima", spiega lo studioso che ha dato alle stampe insieme al sociologo Aldo Bonomi il saggio *Dalla smart city alla smart land*, (ed. Marsilio). "Tutti hanno paura del digitale perché apre al post umano, pensiamo alla robotica, senza capire o immaginare che non c'è nulla di più umano che dialogare con un robot".

Professore non tutti hanno compreso le connotazioni del mondo di oggi. Siamo dentro il flusso di una trasformazione epocale.* Smart, *parola tematizzata nel suo ultimo saggio, è il termine emblematico di questo "cambio di marcia", un termine che trae origine dal fortunato modello di un'automobile, simbolo di quella modernità industriale che fa parte del passato. Questa contraddizione non Le appare quanto meno strana?

Tempo fa Confindustria mi ha chiesto di spiegare ad un vasto pubblico di ragazzi delle scuole superiori, fatti venire da tutta Italia a Venezia per gli esiti di un concorso nazionale, che cosa significasse *smart*. Ero imbarazzato. Non potevo di certo fare una dissertazione accademica a dei ragazzi che avevano principalmente voglia di fare festa. Ho scelto di evocare un episodio di Guerre Stellari sperando che i più se lo ricordassero: Luke Skywalker si ritrova con la sua astronave intrappolato in una palude di un pianeta a lui sconosciuto. Non sa come venirne fuori. Si presenta uno strano omino verde. È il maestro Yoda. Luke Skywalker chiede aiuto e l'omino dice: "No provare, fare o non fare" e prosegue incalzando: "…e soprattutto disimparare". Questa è la sintesi dell'essere smart. "No provare, fare o non fare" significa che non hai alibi e che non puoi tenerti in tasca nessuna scusa: *"Ci ho provato… ma non ce l'ho fatta"*. Significa anche accettare il fatto che solo facendo puoi pensare a come uscirne.

In una parola potremmo usare il motto: non mollare mai?

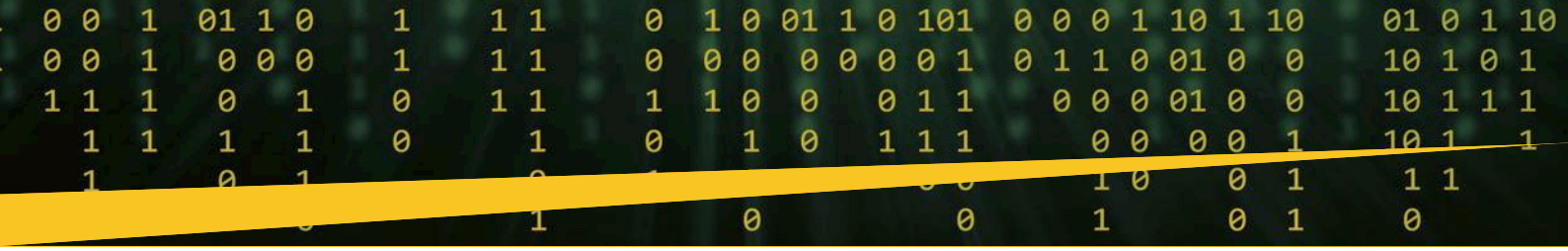
Bisogna continuamente intrecciare quello che chiamiamo teoria con la prassi. La parola chiave forse è fattualità: un pensare che agisce e un agire che pensa. "Disimparare" significa che se non trovi la soluzione al tuo problema vuol dire che ciò che hai imparato è in quel frangente del tutto inutile e quindi non puoi affidarti a ciò che già sai, ma devi elaborare un sapere per quella specifica situazione. Questo è l'atteggiamento smart. Verrebbe da pensare che siamo nella tradizione del pragmatismo americano, quello per intenderci di Emerson, James o Dewey, o quello del libro di Robert M. Pirsig, *Lo Zen e l'arte della manutenzione della motocicletta*, scritto che risale allo stesso periodo. C'è una questione che mi preme molto sottolineare.

Prego, la ascolto con interesse…

Soprattutto in Italia si è pensato che smart fosse una questione tecnologica. Ad esempio *smart cities* significava dotare i lampioni pubblici di pannelli solari o controllare con sensori la differenziata e via immaginando. Essere smart non definisce esclusivamente una tecnologia. Direi di più: anche il digitale non è questione né tecnica, né tecnologica, è un modo di essere, o per dirla in termini filosofici, una questione epistemologica e persino ontologica.

In questo numero di Cyber Security Trends la sua intervista è affiancata da una testimonianza di Carlo Ratti che parla della* "città del futuro". *Proviamo ad affrontare questo aspetto: come saranno i centri urbani di domani? Riusciremo a governare la complessità crescente che segna la contemporaneità?

La domanda presuppone che il problema della complessità appartenga alla dimensione del Contemporaneo e quindi fa pensare che nei tempi passati ci fosse un mondo meno complesso. Non la penso così: la complessità accompagna continuamente la nostra evoluzione. Non solo, ciò che mi affascina della logica di Boole, che sta alla base del digitale, è il fatto che si possa riuscire a produrre una calcolabilità del mondo attraverso la riduzione del complesso al semplice, detto in altri termini si può passare dalle infinite variazione dell'esistente alla coppia logica 0/1. Alle volte arrivo a pensare che il digitale da una parte apra ad un futuro imprevedibile, dall'altra ci faccia tornare a dinamiche cognitive e fattuali previe, originali, che precedono il *logos* occidentale, semplici (anche se solo apparentemente). Venendo alla definizione di città posso dire con franchezza che capisco con difficoltà cosa



intendiamo quando usiamo questa parola. Certo, vale ancora molto per noi Occidentali perché profondamente attaccati alla nostra storia che è fatta di città e solo in parte per le culture in qualche modo legate alla nostra storia, ma il mondo oggi, i processi di aggregazione sociale del nostro tempo e in questo nostro mondo, non sono più quelli. Mi spiego meglio: non esistendo più la distinzione tra città e campagna, tutto e ovunque è diventato *sprawl*, città diffusa, ammasso informe. Non esiste più nessun luogo della terra che non sia stato antropizzato e non ci siano i jeans e la coca cola.

Ha forse nostalgia del passato?

Sia chiaro! Nessuna nostalgia. Quando leggo i dati previsionali sul 2030 secondo i quali l'ottanta per cento della popolazione che allora sarà di otto miliardi e seicento milioni vivrà in città, faccio fatica a immaginare dove vivrà l'altro 20 per cento visto che la campagna non esiste più o per lo meno è e sarà sempre più industrializzata (meglio: bioindustrializzata e digitalizzata). E poi come si fa a parlare di città quando nel mondo si sono formate almeno cinquanta megalopoli con un numero di abitanti spropositato, dai sessanta ai cento milioni. Pensate di poter chiedere dove è la piazza principale, dove sta il municipio? Queste megalopoli trapassano i confini tradizionali di ciò che sino ad oggi abbiamo chiamato non solo città ma anche nazione. Pensate che queste realtà non chiederanno di avere la propria identità politica? E in che forma? Possiamo ancora chiamare città agglomerati che hanno immani dimensioni? Basti questo elenco aggiornato al 2018: Shangai 27 milioni di abitanti, Karachi 23,5, Pechino 21,5, Lagos 21,3, Delhi 16,3, Tientsin 15,2, Istanbul 14,1. Ad alcune la storia ha regalato qualcosa che assomiglia ad un centro città, cioè ad una rappresentazione dei poteri pubblici, per altro grazie all'architettura, ma è solo un caso e non certo la condizione di esistenza economica, politica e sociale delle stesse. E comunque vale ricordare un adagio di Hegel: cambiando la quantità cambia anche la qualità e (dico io) forse anche il nome.

Il futuro prossimo venturo

Resta il fatto che bisognerà cercare di capire cosa accadrà nel prossimo futuro se si vuole affrontare un processo di sviluppo sostenibile, non crede?

A processi di aggregazione così diversificati corrispondono inevitabilmente strategie politiche altrettanto diversificate e sempre più conflittuali sia rispetto all'utilizzo delle risorse sia nelle forme stesse di potere che inevitabilmente si vengono a comporre e a legittimare. Questione non di poco conto. L'Unione Europea ha in questi ultimi anni investito molto sulle città in nome della propria civilissima tradizione urbana (la nostra stessa civiltà – quella occidentale – è fatta di Città: Atene, Roma, Parigi…). Lo ha fatto attraverso i finanziamenti 2014-2020 sulle *smart cities* e sulle *smart communities* proponendo un modello capace di ricomporre le identità urbane attraverso strategie per l'inclusione, l'intelligenza delle *governance* e delle *policy* e la sostenibilità in un quadro di economia circolare. Questo modello, ripeto, civilissimo che ha dato qua e là in Europa notevoli risultati (dei quali daremo conto in una prossima pubblicazione grazie al lavoro fatto da Federico Della Puppa che ha analizzato le città europee in questo senso più virtuose) è difficilmente esportabile, ma appare comunque una risposta alle dinamiche della *deregulation* globale. È in qualche modo una affermazione di civiltà. È comunque una questione "politicissima" che va capita nelle sue dinamiche che sono: inclusione, smart, sostenibilità. La città futura (nella sua visione europea) sarà città solo se inclusiva, smart, sostenibile. E soprattutto se sarà capace di essere una piattaforma di articolati e diversificati interessi capaci di interagire tra il locale e il globale. Quindi l'organizzazione politico-gestionale non può che cercare delle configurazioni totalmente diverse rispetto a quelle tradizionali della mediazione politico-partitica.

BIO

Professore Ordinario di Storia dell'Architettura nell'Istituto Universitario di Architettura di Venezia, Roberto Masiero è studioso delle arti e delle scienze nel quadro di una generale storia delle idee e della politica. Ha insegnato anche nell'Università di Genova e di Trieste. Ha contribuito alla nascita della Facoltà di Architettura di Trieste e della facoltà Design e Arti dell'IUAV, della quale è stato anche Vicepreside. È stato responsabile per l'UE di un Osservatorio sulle Accademie d'arte, Facoltà di Architettura e Ingegneria in Europa. Dal 2014 collabora con *Italiadecide* sul tema del rapporto tra *governance* e mondo digitale. Fa parte del Comitato direttivo della Fondazione Collodi e nel Comitato scientifico della Fondazione Francesco Fabbri per la quale, in particolare, segue il Laboratorio Politico con Quaderni come: *Pensare l'Europa; Riflessioni sulla crisi; Gli spazi della politica* e con la pubblicazione di un *Manifesto per lo smart land* (con F. Della Puppa), uno sulla *Società circolare/ Economia digitale* (con A. Bonomi e F. Della Puppa). Attualmente sta scrivendo un testo sul passaggio dal modo di produzione industriale al modo di produzione digitale dal titolo (provvisorio) *Dopo la tecnica* e sta lavorando a un folder su *Internet di tutte le cose.* (Università di Udine, Eurotech e Fondazione Fabbri).

Cosa vuol dire in concreto e che peso avrà la componente tecnologica in questa prospettiva?

Lasciamo in sospeso tutto il possibile indotto dall'IoT (Internet of Things) o delle applicazioni possibili nei vari settori della gestione pubblica che saranno più invasivi di quanto si pensi. L'IoT non è il domani. È già l'oggi. È comunque urgente valutare cosa potrà accadere della mobilità sia urbana che territoriale. Mobilità che modificherà non nel lungo periodo, ma nel breve, gli assetti spaziali (e quindi le città e i territori) e per molti aspetti, anche i modi di vita e le relazioni sociali.

Immaginate banalmente cosa accadrà nel momento nel quale nessuno comprerà per sé una automobile, visto che potrà con il proprio iPhone chiamarne una di servizio autoguidata alla quale ordinare: portami di qua o di là. Fantascienza? Assolutamente no! Il processo è già in atto ed è velocissimo. Cosa accadrà delle strade, delle autostrade, degli spazi pubblici? Avremmo ancora bisogno dei *garage*? E cosa succederà delle relazioni intersoggettive quando i bambini potranno liberamente giocare negli spazi pubblici non essendoci più il pericolo delle automobili? Sembrano cose banali, ma non lo sono affatto: cambiano i rapporti tra le persone e i modi di vivere. Le città europee studiate da Federico della Puppa, sono cambiate radicalmente proprio perché sono state espulse dagli abitati le automobili privilegiando la mobilità pubblica o l'uso delle biciclette.

Dovremo dunque abituarci a reggere l'impatto con una trasformazione così profonda?

Profonda e inevitabile aggiungerei. Pensiamo a cosa succederà nel momento nel quale – e anche questo accadrà tra poco tempo – potremmo entrare in un negozio per acquistare un oggetto che ci piace e il commesso ci chiede di aspettare per produrlo con la stampante 3D, magari con delle varianti a nostro piacere? Quel negozio avrà un magazzino? Certamente no! e forse nemmeno un commesso, ma potremmo dialogare con un robot. Fantascienza si dirà. Assolutamente no! Si guardino in internet le interviste a Sophie. La stupefacente velocità dei cambiamenti nei modi di produzione, distribuzione e scambio e della conseguente modalità dei consumi privati e collettivi, prevede anche una più veloce capacità di prefigurazione e di progettualità e questo ha bisogno di un pensiero libero (smart) e non di ciò che "resiste". Il vero pericolo oggi è ciò che resiste che, ahimè! sta in tutti noi.

Sicurezza e società del rischio

La nostra rivista si occupa di Sicurezza informatica. Vorrei dunque insistere su questo aspetto.* "Società del rischio" *è la celebre definizione di Ulrich Beck. Possibile che la società di Internet sia più vulnerabile? Per attuare un'efficace* governance *della sicurezza di quali competenze e strutture bisognerà dotarsi?

La mia riflessione è in questa fase prevalentemente orientata sui pericoli che sono legati al predominio del modo di produzione digitale, più che sulle questioni connesse alla sicurezza informatica, intesa nell'accezione più strettamente tecnica. Sono dell'idea che siamo governati dal modo di produzione digitale (che non significa che il modo di produzione industriale non ci sia più o sia destinato a finire, significa semplicemente che i processi di valorizzazione non vengono più determinati dalle logiche della produzione industriale che era prevalentemente fondata sul trasferimento tecnologico, ma dalla formazione dei valori all'interno del modo di produzione digitale che ha come motore il trasferimento dei saperi, cioè l'immateriale). Se questo è il "quadro" il problema diviene: possiamo sentirci sicuri? quali sono i rischi che stiamo correndo nel digitale e che fare, eventualmente, per governare il tutto? Continuo a schematizzare per capirci. Dobbiamo chiederci insomma quali sono i pericoli del "dominio" del modo di produzione digitale, che ritengo sia inarrestabile.

Proviamo in sintesi ad esplicitare quali sono le criticità da affrontare?

Il primo pericolo è "segnato" da un movimento culturale e scientifico (va detto) che è sintetizzato dalla parola "singolarità" proposta da Raymond Kurweil, che prefigura, sulla base della legge di Moore, che pressappoco nel 2040 la capacità di calcolo di un sistema artificiale possa essere superiore a quello del cervello umano e quindi possa in qualche modo auto-svilupparsi producendo la propria stessa evoluzione sino al punto da considerare gli umani e il loro mondo semplicemente superato, se non superfluo, o come risultato di intelligenza oggettivamente inferiore. Mi rendo conto che possa sembrare una provocazione intellettuale, ma sta di fatto che già oggi ci sono intelligenze artificiali che sono di poco inferiori, come capacità di calcolo, a quella di noi umani. La tesi di molti che aderiscono all'idea della *singolarità* è che dobbiamo predisporci ad un patto con l'intelligenza artificiale o, se vogliamo, ad un nuovo patto tra natura e artificio. Qui esiste un oggettivo pericolo, anche se è tutto nelle nostre mani.

I rischi però non finiscono qui, mi pare di aver capito…

No, perché va preso in esame un pericolo più vicino alla nostra dimensione quotidiana: è il pericolo di continuare ad utilizzare modi di pensare, categorie, argomentazioni, convinzioni che nulla hanno a che vedere con ciò che è dominante: il modo di produzione digitale, appunto. È difficile governare e tanto meno combattere ciò che non si conosce o giocare una partita senza conoscere le regole. Questo non significa che non si possa dissentire, ma eventualmente lo si dovrebbe fare conoscendo perfettamente il nemico, cosa che mi sembra di là da venire, ammesso che il digitale sia un nemico.

Più in generale non crede che vada preso in esame il tema della sicurezza intesa sia come sicurezza fisica che ideologica, sia privata che collettiva?

Su questo posso fare una serie di considerazioni a fronte di un fatto: Un programma della Dragonfly Eye cinese lavora con e su 1,7 miliardi di ritratti archiviati in una banca dati. Sono le foto dell'intera popolazione cinese e dei 320 milioni di stranieri fotografati alle frontiere. Ognuno di questi soggetti è non solo identificabile, ma anche localizzabile abbinando l'immagine a tecniche georeferenziali. Nella città di Zhengzhou la polizia usa degli occhiali con telecamera che grazie ad algoritmi di riconoscimento facciale rivela in tempo reale l'identità e varie informazioni di chi sta controllando. È chiaro che il riconoscimento dei volti, come, ad esempio, delle targhe delle auto, può garantire sicurezza e controllo sociale, ma altrettanto chiaro che questa invasione sulla privacy può diventare un terribile strumento antidemocratico: il potere può sapere tutto di tutti, e indubbiamente questa è cosa molto, molto pericolosa. Un così radicale controllo sociale ha ridotto di molto i fenomeni malavitosi e la stessa delinquenza a fronte di una perdita di libertà personale visto che il controllo sociale riguarda inevitabilmente anche il dissenso politico. Inoltre viene messo in discussione il valore della privacy e quindi dell'autonomia e dell'identità di ogni singolo soggetto. Direi di più: quello che viene messo in discussione è il concetto stesso di soggettività. Che posizione prendere? Rifiutare l'utile di queste tecnologie? Dubito che serva a qualcosa visto che le tecnologie hanno sempre vinto e in più c'è il fatto che, come detto in precedenza, il digitale non è una tecnologia, ma un modo d'essere che ha già, volenti o nolenti, configurato l'intero pianeta e non solo.

Come se ne esce?

È necessario in tempi molto veloci ripensare radicalmente sia la politica che la giurisprudenza, meglio lo stesso *diritto* privato e pubblico, pensando in modo digitale o smart, che dir si voglia. Si può fare, meglio si deve fare, altrimenti vincerà il grande fratello, cioè il nostro modo di resistere a fronte non solo di ciò che viene, ma che è anche già avvenuto. Si tenga presente la connotazione *social* del digitale che dimostra come il problema non sia il digitale, ma l'uso che ne sappiamo fare collettivamente. Come sempre in un delitto la colpa non è dell'arma, ma di chi compie il delitto. In questo caso si tratterebbe di un vero e proprio suicidio.

Cambia l'economia e con essa le regole e i valori di riferimento

Il confronto tanto dibattuto tra industriale e digitale come va argomentato in maniera corretta?

Quando cambia un modo di produzione cambia tutto, decisamente tutto. Cambia l'economia, la politica, la formazione dei valori (non solo quelli economici),

i rapporti sociali e quindi l'etica e l'estetica, cambia la visione del mondo e quindi l'epistemologia, cambia anche la stessa soggettività o l'idea fattuale che abbiamo su di noi, cambia la percezione dello spazio e del tempo e quindi cambiano i complessi sistemi dell'organizzazione sociale e inevitabilmente l'uso che facciamo dello spazio e del tempo.

L'economia industriale era per propria natura lineare, progressiva, comandata, burocratizzata, iperdeterminata e ipercontrollata e fondata sulle logiche standard. Il sistema era fondamentalmente proprietario. L'economia governata dal digitale è, di contro, circolare, fondata su logiche di feedback, è fortemente relazionale, attiva processi di *disruption* e il valore aggiunto delle merci come dei servizi è caratterizzato da una forte componente intellettuale e sociale. Pratica in modo sempre più diffuso l'*open source*, lo *sharing* e il *peer to peer*. Il conflitto sociale si configura tra capitale e intelligenza collettiva. La questione cruciale diventa la biopolitica cioè, accettato il welfare, la questione diventa la "buona vita". Il sistema tende ad essere collettivo. La rottura è molto forte rispetto al passato. La società industriale di tipo lineare, produce prodotti, la società digitale, circolare, processi. E così anche le dimensioni territoriali, ambientali, paesaggistiche non si configurano più come prodotti, ma come processi, nella logica di piattaforme, *Hub*, e come tali vanno governati in modalità digitale.

Siamo dunque immersi in un contesto che presenta dinamiche, linguaggi e visione del mondo specifiche?

La società digitale è strutturata non sull'"io", ma sul "noi", una società interconnessa in cui ogni soggetto è uno "stato di relazione". Si configura attorno a tre modalità sostanzialmente immateriali: internet, Big data e Cloud che aprono ad un sistema di produzione, distribuzione, scambi e consumo nei modi dell'IoT, meglio *dell'internet of everything*. L'intero sistema economico si sta ristrutturando nelle forme dell'economia circolare, dell'*eco innovation*, della *green economy* e *industrial ecology* e soprattutto nella *disruption innovation*, che stanno modificando radicalmente il modo di fare business. La conseguenza è che la finanza e i processi di valorizzazione non dipendono più da quello che veniva chiamato l'equivalente generale o dal valore delle riserve auree degli Stati, ma operano nelle logiche del *peer to peer*, dell'*open source*, della *sharing economy*, del *crowdfounding* e *crowdlending*. Il digitale sta modificando le forme della stessa transazione economica e va progressivamente verso una demonetizzazione della transazione economica

Le élite sono preparate per compiere questo salto di visione e di cultura?

Maledettamente no! E questo è proprio un guaio. Come intervenire? rivedendo nel loro insieme i sistemi formativi e, contemporaneamente, elaborando una strategia per la formazione e selezione della classe politica.

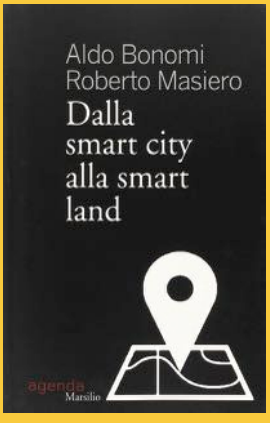
Sul fronte degli stili di vita quali saranno gli atteggiamenti dominanti?

Basta guardarsi attorno per capire che sono decisamente cambiati. In meglio o in peggio? Sarebbe una domanda sbagliata. Bisognerebbe chiederci quale forma di civiltà stanno configurando e *accompagnarli* affinché non diventino autodistruttivi. ■

Cosa vuol dire essere Smart

Essere continuamente in gioco, essere in uno stato permanente di relazione, quindi in rete.
Nella relazione, significa essere disponibili sempre per qualcosa di imprevedibile, nel contempo significa che ogni processo cambia nel contesto e per il contesto.
Che ogni fenomeno ha una moltitudine di indotti e che ogni teoria degli indotti, e quindi delle relazioni potenziali, non può che essere anche una pratica. Che i saperi, inevitabilmente e sempre, strutturano e sono in relazione e che quindi non sono altro dalle tecniche.
Significa conoscere le regole del gioco per provare a "spiazzarle". Fare la mossa imprevedibile, visto che nulla può essere dato per scontato.
Significa saper trasformare il complesso in semplice e il semplice in complesso; considerare ogni sintesi a sua volta come processo e come scenario; chiedersi perché un battito di farfalla nelle foreste dell'Orinoco può determinare una tempesta a Tokio.
Sapere che l'intelligenza è potente quando è strategica; che possiamo essere liberi perché l'intelligenza, quella collettiva, ce lo permette; che per fare arte non necessariamente ci vogliono gli artisti; che la conoscenza come la creatività sono inevitabilmente pubblici e relazionali; che le cose ci parlano e che quindi "forse" pensano (di fatto l'intelligenza nasce nella relazione con loro).
Che le abitudini come i pregiudizi sono tali perché si possono cambiare; che l'innovazione può essere dovunque, nel micro come nel macro; che le reti sono per propria natura intelligenti e che proprio per questo si possono espandere, ridurre, inventare.
Sapere che tutto ciò che è può essere smart.
Smart significa, in quanto relazione, che tutto è sociale; essere smart significa intrecciare saperi, che tutto si può con-dividere.
Significa immaginare dovunque sensori e attuatori, stimoli e risposte; significa sapere che la tecnica non è il tutto, ma che può risolvere tutto.
Che la suddivisone tra soft e hard è fondamentale ma non necessaria; che il soft può continuamente reinventare l'hard e se stesso; smart significa mette in relazione il grande e il piccolo.
Smart è glocale.
Smart non è puntare sulla competitività ma sulla inclusione: collaborare anziché competere.
Smart è, per propria disposizione, politica.
E forse essere smart significa provare ad essere (mentalmente) liberi.

Tratto da
Aldo Bonomi, Roberto Masiero
"Dalla smart city alla smart land"
Marsilio



Smart Land

da **Smart City** ⟶ a la città che agisce attivamente per migliorare la qualità della vita dei propri cittadini

Smart Land
(come costruire) un territorio sostenibile, intelligente, inclusivo

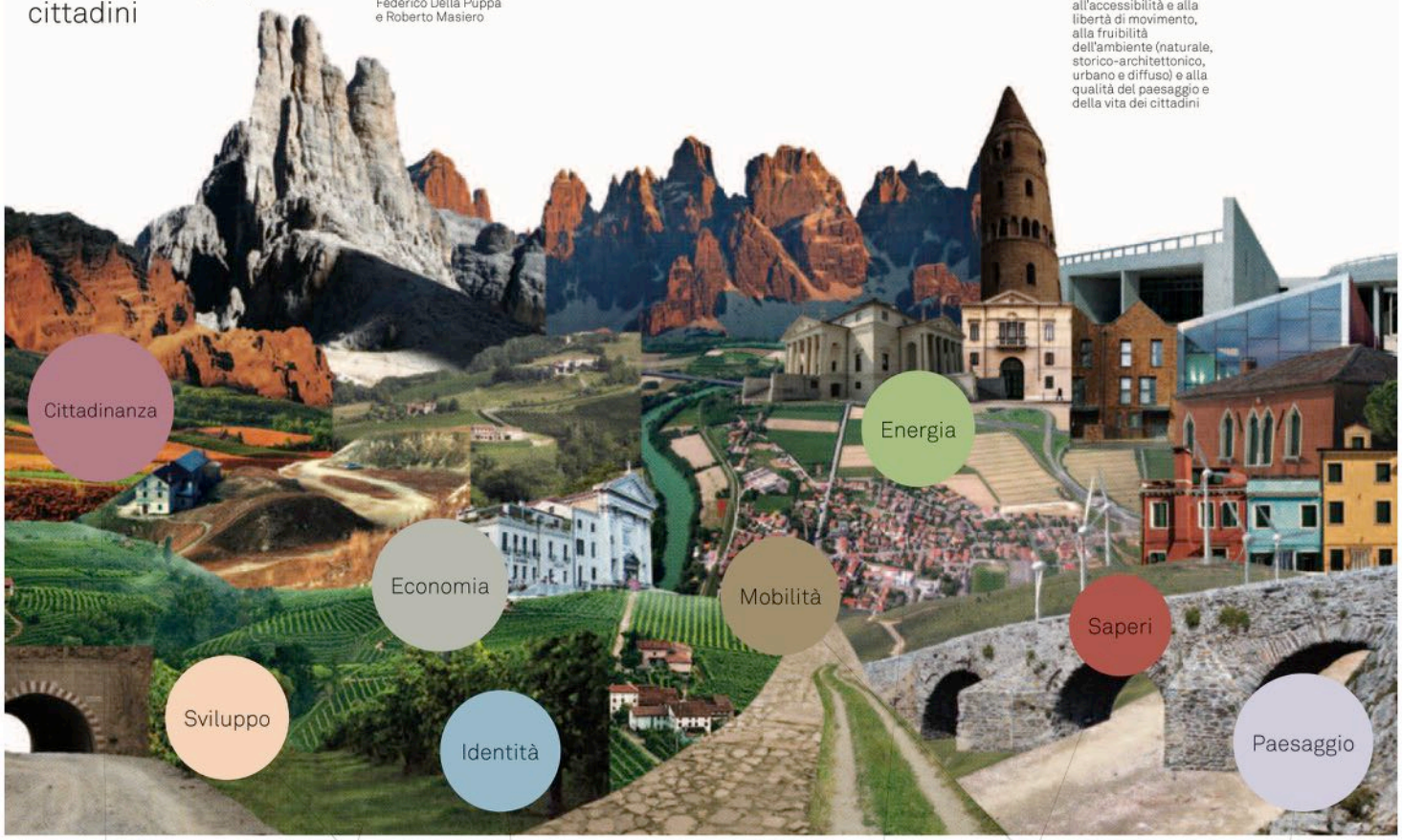
A cura di
Federico Della Puppa
e Roberto Masiero

A chi è destinato

Un manifesto dedicato a politici, amministratori, stakeholders, categorie professionali, movimenti, associazioni e cittadini per promuovere una nuova politica di sviluppo basata sulla qualità della vita non solo nelle città ma anche nei territori diffusi

Cosa significa Smart Land

Uno smart land è un ambito territoriale nel quale attraverso politiche diffuse e condivise si aumenta la competitività e attrattività del territorio, con una attenzione particolare alla coesione sociale, alla diffusione della conoscenza, alla crescita creativa, all'accessibilità e alla libertà di movimento, alla fruibilità dell'ambiente (naturale, storico-architettonico, urbano e diffuso) e alla qualità del paesaggio e della vita dei cittadini



Cittadinanza

Uno smart Land è un luogo nel quale la cittadinanza si fa attiva e nel quale le forme di partecipazione e condivisione dal basso di progetti di sviluppo va di pari passo con una nuova modalità di interazione e integrazione tra amministratori e forze locali, siano essi portatori di interesse, movimenti o associazioni o semplici cittadini.

Si tratta di applicare nella sua forma più estesa il principio di sussidiarietà previsto dalla stessa costituzione italiana che pretende che le decisioni che riguardino il bene pubblico da parte delle istituzioni, e quindi anche dalla politica, debbano essere socialmente condivise. Questo, grazie alle tecnologie digitali, è oggi più che possibile. Tali decisioni vanno considerate rispetto alla loro capacità di inclusione: i cittadini non possono essere considerati sudditi.

Azioni:
• integrare i cittadini nella distribuzione delle informazioni e del sapere, in una logica di long life learning, mediante le nuove tecnologie, attraverso la costruzione di reti informative capillari, e attraverso azioni di alfabetizzazione informatica diffusa.

• promuovere l'integrazione culturale inter e intragenerazionale, nonché sociale ed etnica, attraverso l'interscambio culturale e la promozione di azioni di cittadinanza attiva mediante coinvolgimento delle associazioni di cittadini, dei gruppi sociali e dei singoli

• creare le condizioni per promuovere la coesione e l'inclusione sociale, eliminando le barriere fisiche, sociali e culturali che impediscono la completa accessibilità per tutti i cittadini

Sviluppo

In uno smart Land lo sviluppo avviene attraverso la costruzione di una rete delle reti diffuse, nella quale i diversi portatori di interesse e le comunità possono svolgere un ruolo attivo, sviluppando progetti, programmi e processi nei quali il punto nodale è il sapere diffuso e condiviso, che le imprese possono utilizzare per aumentare la propria competitività e capaxità di creare occupazione a livello locale, oltre alla promozione del territorio quale bene comune da preservare e valorizzare ai fini culturali e turistici, garantendone la fruibilità e ottimizzando i flussi.

L'elaborazione strategica delle linee di sviluppo non deve essere formulate su criteri meramente economici, ma pertendo da una visione nel lungo periodo del benessere collettivo e della difesa dei diritti dei cittadini. E' fondamentale il coinvolgimento di tutti i soggetti nel promuovere cambiamento e sviluppo.

Azioni:
• produrre un piano strategico di sviluppo, nel quale siano evidenziate e declinate tutte le politiche inerenti la realizzazione dello smart land a livello locale, definendo attraverso un percorso partecipativo e condiviso la vision, gli obiettivi e le specifiche linee di azione, associate alle potenzialità di finanziamento

• promuovere attivamente lo sviluppo sostenibile, supportando a livello locale le politiche attive europee e nazionali e integrandole con specifiche misure e azioni di incentivazione a livello comunale

• sviluppare allenze strategiche con le università, con le agenzie formative formali e informali e con soggetti specializzati al fine di promuovere la crescita a livello locale dell'economia della conoscenza

• valorizzare il patrimonio culturale (ambientale, storico, architettonico, dei saperi e dei mestieri) e le proprie tradizioni e restituirla in rete come "bene comune" per i propri cittadini e i propri visitatori

• creare ambienti favorevoli all'insediamento di nuove imprese e di start up innovative legate alle nuove professioni nel campo della creatività e della conoscenza

Energia

In uno smart Land la produzione e la gestione dell'energia deve essere diffusa e articolata, utilizzando tutti i sistemi più innovativi legati alle smart grids e alle reti diffuse, promuovendo azioni di cogenerazione e di genrazione distribuita, facilitando gli investimenti nelle energie rinnovabili e promuovendo azioni di utilizzazione razionale dell'energia, puntando sul risparmio energetico a tutti i livelli, dagli edifici pubblici a quelli privati

Il principio fondamentale è sviluppare tutte le forme di energia alternative e rinnovabile e, soprattutto, ottenere come risultato che tutti gli indotti economici e sociali rimangano nei territori di produzione. Questo è possibile ad esempio promuovendo piani territoriali energetici affidati a soggetti pubblici e privati sulla base di accordi territoriali attivando contemporaneamente in questo settore processi di start up e quindi di nuova imprenditorialità.

Azioni:
• mobilitare le forze economiche e sociali verso politiche energetiche virtuose, lavorando con i soggetti interessati al fine di implementare scelte di efficienza energetica a livello locale attraverso "long-term committment", ovvero impegni su programmi di intervento a lungo termine, come ad esempio il Patto dei Sindaci, che fornisce anche risorse per realizzare tali politiche

• razionalizzare i consumi elettrici a partire dall'illuminazione pubblica e privatiovendo l'efficienza energetica in edilizia per abbattere i consumi e l'impatto negativo del riscaldamento e della climatizzazione

• ridurre le emissioni di gas serra tramite la limitazione del traffico privato e promuovendo una riduzione/ottimizzazione delle emissioni industriali, attraverso la realizzazione di sistemi di gestione dell'energia e dei rifiuti innovativi (come le APEA, aree produttive ecologicamente attrezzate)

• ridurre l'ammontare dei rifiuti, incrementando la raccolta differenziata e valorizzando economicamente la filiera del riciclo

Mobilità

Uno smart Land è un luogo dove gli spostamenti sono facili, agevoli, dove il trasporto pubblico cresce nella qualità dei servizi, mettendo a disposizione mezzi a basso impatto ambientale e dove vengono realizzati e facilitati i percorsi della mobilità alternativa al trasporto privato e dove vengono realizzati sistemi di traffic calming nei centri storici delle città, dei borghi e dei nuclei abitati e nel quale le nuove infrastrutture sono affiancate da infostrutture in grado di promuovere una migliore accessibilità dei cittadini con le aree limitrofe e con le reti della grande mobilità extraurbana

Definire il piano urbano della mobilità, ottimizzando la rete viaria esistente e agevolando i percorsi casa-scuola e casa-lavoro, regolamentando l'accesso al centro storico e privilegiando la vivibilità, con la creazione di aree pedonalizzate e sistemi di traffic calming in grado di ridurre la velocità di attraversamento dei centri abitati.

Azioni:
• garantire una adeguata disponibilità di trasporto pubblico innovativo e sostenibile, promuovendo l'uso di mezzi a basso impatto ecologico, in primo luogo la bicicletta, attraverso la realizzazione di postazioni di bike sharing associate a parcheggi decentrati

• adottare soluzioni avanzate di mobility management che consentano di investare i flussi locali anche sulle grandi vie di comunicazione, senza incrementare ulteriormente la pressione dei mezzi privati, ma favorendo azioni di car sharing e car pooling, mediante adeguate campagne di educazione alla condivisione dei mezzi di trasporto privati

• implementare sistemi avanzati di comunicazione e informazione che permettano lo scambio informativo sulla mobilità sia tra amministrazione e cittadini, sia tra i cittadini stessi (infosharing)

Economia

In un territorio smart l'economia si sviluppa soprattutto attraverso sistemi di interazione tra cittadini e imprese, tali che si produca un meccanismo di appendimento continuo e di forte interazione tra sistema della formazione e imprenditorialità, con particolare attenzione allo sviluppo della creatività, del sostegno alla formazione di start up, facilitando la creazione di laboratori di idee

Fondamentale è la diffusione di incubatori di imprese, sviluppare i processi tenendo conto delle direttive dell'Agenzia digitale, incentivare creatività e conoscenza collettive; integrare il mondo della tradizione con le nuove tecnologie cercando in esse le forme stesse dello sviluppo; coinvolgere tutti i soggetti e in particolare il sistema bancario in questi processi. Ogni fenomeno locale è oggi globale; ogni fenomeno globale è oggi locale.

Azioni:
• valorizzare il tessuto produttivo esistente, favorendo azioni di ottimizzazione dei servizi a supporto delle imprese e, dove possibile, realizzando aree produttive ecologicamente attrezzate (APEA), seguendo le linee guida europee e quelle del Ministero dell'Ambiente, al fine di creare un ambiente favorevole alle PMI e alle start up, con servizi e spazi dedicati

• supportare le imprese nella riconversione produttiva verso prodotti e sistemi produttivi ecocompatibili, seguendo le direttive europee relative a ETAP ed ECOAP, sulla base delle linee guida del Ministero dell'Ambiente

• garantire a tutti l'accessibilità alle reti informatiche e tecnologiche, agendo a livello di governance su accordi con i fornitori dei servizi per creare un ambiente adeguato alla competitività, alla creatività, all'inclusività nelle reti sociali, coinvolgendo i portatori di interesse e le comunità locali

• promuovere la riqualificazione e il rinnovo, nonché la manutenzione attiva dell'esistente, in termini di incremento qualitativo, di risparmio energetico e di miglioramento del benessere e della qualità della vita

Identità

Uno smart Land è un luogo identitario, nel quale le diverse identità territoriali – ambientali, artigianali, culturali, economiche, paesaggistiche, produttive – possono esprimersi al massimo della propria capacità, trovando adeguata valorizzazione in un sistema di offerta che utilizzi sistemi avanzati per promuovere percorsi, mappature, tematismi che ne valorizzino le specificità e ne aumentino il valore aggiunto e quello percepito

L'identità non può essere il "come eravamo". Deve essere il "come possiamo e vogliamo essere nel futuro" ("sono ciò che sarò"). In questo senso le azioni di intervento devono essere orientate alla costruzione di una identità locale basata sul patrimonio comune, materiale e immateriale, che va valorizzato sia nei suoi aspetti tangibili, che in quelli intangibili.

Azioni:
• valorizzare il patrimonio culturale, dei saperi, dei luoghi e delle proprie tradizioni e restituirle in rete come "bene comune" per i propri cittadini e i propri visitatori

• valorizzare la propria identità privilegiando il riuso e la valorizzazione dell'esistente in un rinnovamento che si basa sulla conservazione e manutenzione dell'esistente, rendendo fruibili i contenuti ambientali, paesaggistici, culturali, sociali, architettonici, storici, urbanistici, produttivi ed economici e qualsiasi elemento che rappresenti il DNA territoriale della comunità, sviluppando dunque i temi della smart community secondo quanto indicato dall'Unione Europea.

• promuovere la propria identità con una presenza intelligente sul web e sui nuovi media, utilizzando tecniche avanzate per creare percorsi e "mappature" tematiche del proprio territorio e rendendole facilmente fruibili

• promuovere un'offerta coordinata ed intelligente della propria offerta turistica sul web, con un uso strategico e attento dei nuovi media e in particolare dei social media

Saperi

Uno smart Land è un luogo nel quale i saperi, la conoscenza e la cultura assumono un significato centrale nelle politiche di sviluppo, mediante la creazione di reti di saperi diffuse e integrate, facilitando la creazione di laboratori di idee e mettendo in sinergia tutte le componenti culturali, produttive e non produttive, dell'artigianato come dell'alta formazione, presenti nel territorio

Attuare ovunque processi di formazione continua, di aggiornamento delle competenze, di ibridazione fra saperi accademici e non, locali e non, tradizionali e innovativi, coinvolgendo tutti i soggetti formali e informali istituzionali e non istituzionali che possono contribuire allo sviluppo olettivo.

Azioni:
• promuovere attivamente la crescita dell'economia della conoscenza e della tolleranza, come fattori strutturali della produzione di sapere e di incremento della competitività del territorio, sia in senso sociale ed inclusivo, sia in senso economico e produttivo

• promuovere l'apprendimento continuo (life long learning) e percorsi formativi personalizzati

• offrire un ambiente adeguato alla creatività, incentivando le innovazioni e le sperimentazioni nell'arte, nella cultura, nello spettacolo

• incrementare e garantire l'accessibilità alle reti informatiche

• sostenere l'inclusività nelle reti sociali, coinvolgendo i portatori di interesse e le loro comunità, al fine di dare cittadinanza e voce a tutti il patrimonio di saperi che, attraverso la condivisione e le nuove tecnologie, possono essere fonte di crescita culturale, sociale ed economica

• dare spazio, occasioni, strumenti e piattaforme di interazione per promuovere la libera conoscenza, privilegiando le forme di peer-to-peer approach, nelle quali il sapere è libero e diffuso

Paesaggio

Uno smart land è un luogo nel quale l'attenzione al paesaggio non è solo preservazione della bellezza esistente, ma miglioramento dei processi che lo valorizzano, dalla gestione dei rifiuti alla riduzione dei gas serra, dalla limitazione del traffico privato alla riqualificazione urbana e territoriale, secondo modelli orientati alla qualità della vita e dei luoghi, promuovendo il risparmio di suolo, bonificando le aree dismesse e riutilizzandole al fine di migliorare l'offerta territoriale e la fruibilità dei luoghi stessi

Per la Convenzione europea del paesaggio, il paesaggio "...*designa una determinata parte del territorio, così come è percepito dalle popolazione, il cui carattere deriva dall'azione di fattori naturali e/o umani e dalle loro interrelazioni*". Essa prevede di considerare tutti i paesaggi indipendentemente da prestabiliti canoni di bellezza o originalità ed include espressamente "...*paesaggi terrestri, le acque interne e marine. Concerne sia paesaggi che possono essere considerati eccezionali, sia paesaggi della vita quotidiana, sia i paesaggi degradati*". La Convenzione Europea sul Paesaggio apre a quello che può essere considerata la nuova etica per il terzo millennio, in quanto prevede il principio dell'eguale dignità e del necessario rispetto di tutte le culture e del fatto che queste culture sono intimamente legate al proprio territorio, al proprio ambiente, al proprio paesaggio.

Azioni:
• ridurre il consumo di suolo e promuovere la valorizzazione del paesaggio come elemento fondante dell'identità territoriale, attraverso specifiche norme nei regolamenti di gestione delle aree territoriali comunali, anche attraverso forme innovative di tutela e conservazione

• promuovere, proteggere, incrementare e gestire il verde urbano

• bonificare e recuperare le aree dismesse, secondo i modelli europei della riqualificazione urbana, ambientale e sociale promossa dall'acquis urban e dai nuovi modelli di intervento della futura programmazione 2014-2020

Smart City

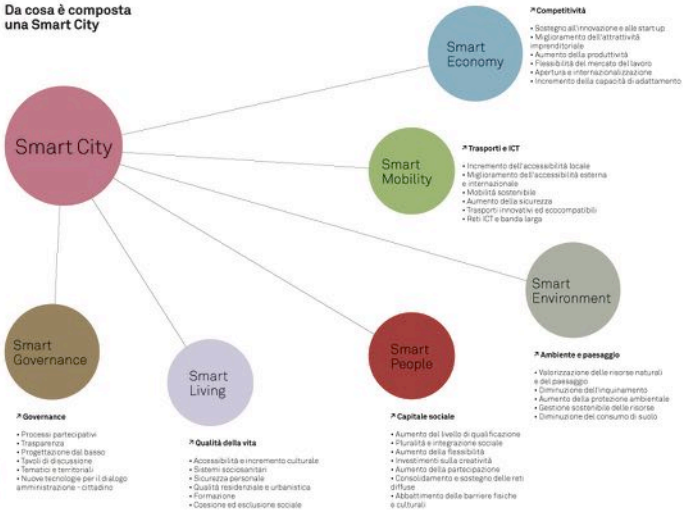
Smart City

La smart city è la città del futuro, dove con meno risorse si producono più servizi per i cittadini e per le imprese, utilizzando le tecnologie più avanzate e sistemi di gestione intelligenti per ridurre gli sprechi e gli impatti negativi, siano essi ambientali, economici, sociali.
In una smart city c'è meno inquinamento, si producono meno rifiuti e quelli prodotti sono riutilizzati per ridurre l'uso di materie prime, si consuma meno energia producendola con fonti rinnovabili, si riduce il traffico aumentando il trasporto pubblico e quello alternativo, si riduce l'uso di mezzi privati incrementando la condivisione dei mezzi, facilitando la diffusione del bike sharing, del car sharing, del car pooling, si riduce l'esclusione sociale mediante politiche di inclusione attive e attente alle diverse forme di bisogni, si abbassano le disparità di accesso ai servizi e all'uso della città stessa, si riducono le barriere architettoniche, quelle fisiche e quelle culturali. La smart city è una città che usa l'intelligenza delle nuove tecnologie per costruire un ambiente urbano più sostenibile, il cui esito è un sistema di relazioni inclusivo che attrae, accoglie, accudisce e che accompagna i cittadini a realizzarsi.

La smart city è una città organica, un sistema di sistemi, che nello spazio urbano affronta la sfida della globalizzazione in termini di aumento della competitività, dell'attrattività, dell'inclusività puntando su 6 assi – economia, mobilità, ambiente, persone, qualità della vita e governance – e che attraverso azioni specifiche diventa una città più tecnologica, più interconnessa, più pulita, più attrattiva, più sicura, più accogliente, più efficiente, più aperte e collaborativa, più creativa e più sostenibile.

Use less more

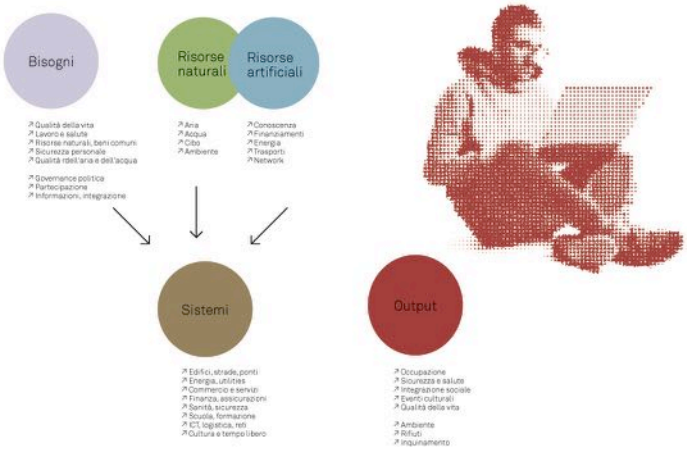
Da cosa è composta una Smart City



Che cosa serve per realizzare una Smart City

Una città intelligente non è un progetto, ma un percorso, un processo che va avviato con il supporto delle tecnologie innovative ed essendo un processo è fondamentale la **governance**, ovvero la costruzione di meccanismi di gestione in grado di ottimizzare il sistema di servizi che una smart city deve offrire (livello minimo di offerta) e che può offrire (livello potenziale di offerta)

Qual è il percorso logico per realizzare una Smart City



5 politiche principali

4 campi di azione prioritari

3 modelli di intervento

Strategia smart 1: Tutto dentro
Il Comune affida ai propri servizi lo studio e la predisposizione delle azioni da realizzare

I servizi/referati definiscono e strutturano i servizi in base a "carte di servizio" che specificano il livello, la dotazione e la qualità dei servizi erogati all'utenza

Tutti i costi di investimento e le eventuali entrate da gestione sono in capo all'Amministrazione Comunale

Gli uffici progettano e realizzano le strutture

Strategia smart 2: Mista
Il Comune affida ai propri servizi lo studio e le azioni da realizzare, avvalendosi di strutture tecniche esterne specializzate

L'Amministrazione Comunale tramite i propri uffici predispone gare per la realizzazione dei lavori e/o per l'affidamento della gestione dei servizi

I costi di investimento sono in capo all'Amministrazione Comunale e si prevedono entrate per canoni da gestione

Gli uffici progettano e/o (laddove utile) realizzano le strutture avvalendosi di consulenze specialistiche esterne (SDF)

Strategia smart 3: Tutto fuori
Il Comune affida i propri servizi e, sulla base di specifiche richieste, lo studio e le azioni da realizzare, avvalendosi di studi di fattibilità da parte di strutture tecniche esterne specializzate

I costi di investimento e le entrate da gestione sono in capo ai realizzatori. Sulla base dei risultati degli studi di fattibilità l'Amministrazione Comunale può fissare canoni concessori eventualmente premianti in relazione ai risultati raggiunti dall'implementazione dei diversi servizi attivati

Attraverso bandi (project financing, manifestazioni di interesse, ecc.) in base alle caratteristiche dei lavori e dei servizi vengono individuati i realizzatori/gestori

Colophon

Questo foglio esemplificativo è stato elaborato all'interno del Laboratorio Politico della Fondazione Francesco Fabbri, coordinato da Roberto Masiero e da Luca Taddio e presentato per la prima volta all'interno del Festival Comodamente del 2013.

Autori:
Federico Della Puppa
Roberto Masiero

Progetto grafico:
Heads Collective

Stampato da:
Europrint, Treviso
2013

Fondazione Francesco Fabbri Onlus

Pieve di Soligheto Tv
31053 Piazza Libertà, 7
m 334 9877348
f 0438 894711
info@ fondazionefrancescofabbri.it
www.fondazionefrancescofabbri.it

http://twitter.com/FFFabbri
www.facebook.com/FondazioneFrancescoFabbri

THEORIMA

Dove si trovano le risorse per realizzare una Smart City

La prima e più importante fonte di finanziamento è l'Unione Europea, con i bandi specifici per le smart cities, legati alla **Smart Cities & Communities European Innovation Partnership (SCC)**, una iniziativa con la quale la Commissione Europea intende stimolare lo sviluppo e l'inserimento delle tecnologie intelligenti nella città, attraverso una serie di progetti dimostrativi, che saranno realizzati in collaborazione con le città stesse, con una dotazione finanziaria complessiva di circa 11 miliardi di euro concentrati sulla riqualificazione energetica degli edifici, sulle reti energetiche e il risparmio energetico e sul miglioramento del sistema della mobilità. A questi fondi, che l'UE gestisce direttamente, sono associati altre tipologie di supporto finanziario per progetti di efficienza energetica e rinnovo urbano i cui contenuti puntano alla realizzazione di Smart Cities, i cui acronimi sono **JESSICA** (Joint European Support for Sustainable Investment in City Areas), **ELENA** (European Local ENergy Assistance), **EEEF** (European Energy Efficiency Facility) e **IEE** (Intelligent Energy Europe). Tutti questi programmi sono legati allo sviluppo delle politiche locali a partire dal **Patto dei Sindaci**, che impegna le amministrazioni a cogliere gli obiettivi di **Europa 2020**, mediante azioni e strumenti coerenti con le politiche di contenimento energetico e di innovazione, dunque smart per le parti legate all'uso della tecnologia. A livello nazionale, vari bandi ministeriali hanno ad oggi promosso azioni di investimenti smart sulla città e altri ne verranno in futuro. Altre modalità di finanziamento vanno ricercate nella capacità di costruire forme di **partenariato pubblico-privato** (PPP) in grado di realizzare politiche smart, costruendo contratti su misura con promotori che, nel miglioramento dell'uso delle risorse e nella gestione di lungo periodo, possano trovare efficienza economica e dunque convenienza ad investire su tali azioni. A livello di gestione energetica, le ESCO (Energy Service Company) oggi sono un valido aiuto per trovare forme di concessione di servizi di gestione in senso smart. Ma il PPP ha varie modalità di applicazione e può essere utilizzato in varie forme per vari scopi, non solo quelli legati alla produzione e gestione dell'energia, dei rifiuti o degli altri servizi pubblici più conosciuti. E' importante che le città e le amministrazioni scelgano il modello di PPP giusto per il progetto da realizzare e potrebbe essere utile strutturare un contratto "su misura", in cui identificare chiaramente le responsabilità tra pubblico e privato, condizione fondamentale per attirare i capitali privati. Gli istituti giuridici alla base di questi modelli possono essere appalti, appalti misti o concessioni di costruzione e gestione o di gestione. Da un punto di vista finanziario, questi modelli possono essere realizzati attraverso differenti strutture, un finanziamento strutturato, in cui l'operatore privato investe mezzi propri e risorse prese a prestito dal sistema bancario; modelli di project financing, in cui un veicolo costituito ad-hoc (che potrebbe essere anche una ESCO) finanzia il progetto con prestiti ricevuti prese a prestito dal sistema bancario (investimento a leva); modelli di leasing finanziario o operativo. Tutti questi modelli di finanziamento possono prevedere anche il cofinanziamento pubblico, utilizzando, per esempio risorse derivanti dai fondi strutturali o da altri fondi. Infine, non vanno dimenticate le donazioni e le nuove forme di raccolta basate sull'impact investing e il crowdfunding.

Dove informarsi

Fonti europee

European Initiative on Smart Cities: http://setis.ec.europa.eu/implementation/technology-roadmap/european-initiative-on-smart-cities

JESSICA (Joint European Support for Sustainable Investment in City Areas): http://ec.europa.eu/regional_policy/thefunds/instruments/jessica_en.cfm

ELENA, sostegno a città e regioni nello sviluppo di soluzioni sostenibili: http://ec.europa.eu/environment/ecoap/about-eco-innovation/policies_matters/eu/33_it.htm

Patto dei Sindaci: http://www.pattodeisindaci.eu

Intelligent Energy Europe (IEE): http://ec.europa.eu/energy/intelligent/

Fondo Europeo per l'Efficienza Energetica (EEEF): http://eeef.eu/home-it.html

The smart city model: http://www.smart-cities.eu/model.html

Fonti nazionali

Programma Operativo Nazionale Ricerca e Competitività: http://www.pongroma.it/programma/interventi/smartcities/

MIUR, Smart Cities and Communities and Social Innovation: http://hubmiur.pubblica.istruzione.it/web/ricerca/smart-cities-and-communities-and-social-innovation

Smart city – Progetti e tecnologie per città più intelligenti: http://lsapori.forumpa.it/story/51416/smart-city-progetti-e-tecnologie-citta-piu-intelligenti

Approfondimenti
Andrea Granelli, Città intelligenti? Per una via italiana alle Smart Cities: http://www.agranelli.net/DIR_rassegna/libro_CittaIntelligenti.html

Michele Vianello, Gestire la complessità urbana nell'era di internet: http://www.acribd.com/doc/126743057/Smart-cities-Gestire-la-complessita-urbana-nell-era-di-Internet

Eleonora Riva Sanseverino, Raffaella Riva Sanseverino, Valentina Vaccaro, Atlante delle smart cities. Modelli di sviluppo sostenibili per città e territori: http://www.franconangeli.it/Ricerca/Scheda_libro.aspx?ID=20812

Fondazione Francesco Fabbri

A cura di:
Aldo Bonomi
Federico Della Puppa
Roberto Masiero

Società circolare → Economia digitale

Dal modo di produzione industriale al modo di produzione digitale

La società che rivede il proprio modello di **sviluppo** → Attraverso il **digitale** costruisce un futuro intelligente, sostenibile e inclusivo.

Smart community
Smart land
Smart city
E-governement

Internet delle cose

Economia

Economia circolare
Industrial ecology
Green economy
Disruption innovation
Eco innovation

Open source
Crowdlending
Sharing economy
Peer2peer
Crowdfounding

Finanza

Internet
Internet of everything

Società interconnessa
IO NOI IO NOI
IO NOI IO NOI
IO NOI IO NOI
IO NOI IO NOI
Società interconnessa

Big Data

Blockchain
Bitcoin

Cloud
Computing

Resilienza
Best practice
Interaction design
Social design
Gamification
Biomimesi

Nuovi modi della transazione economica

Modalità del progetto sociale

Saperi

Il capitalismo cognitivo

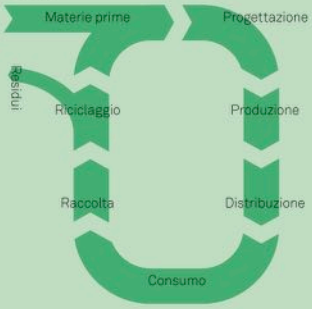
Sostenibilità

Cambiamento di sistema

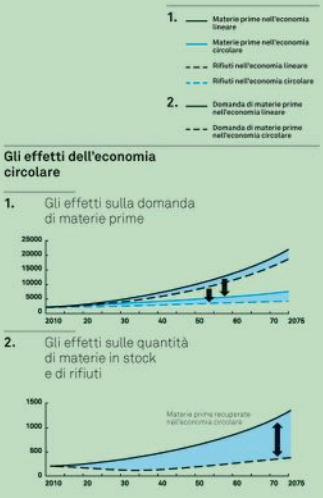
dall' Economia Lineare → all' Economia Circolare

Economia Lineare

Economia Circolare



Gli effetti dell'economia circolare



Come applicare il modello circolare?

Città circolare

Intelligente
Smart

- Conoscenza
- Reti digitali
- Formazione continua

Sostenibile
Ecologica

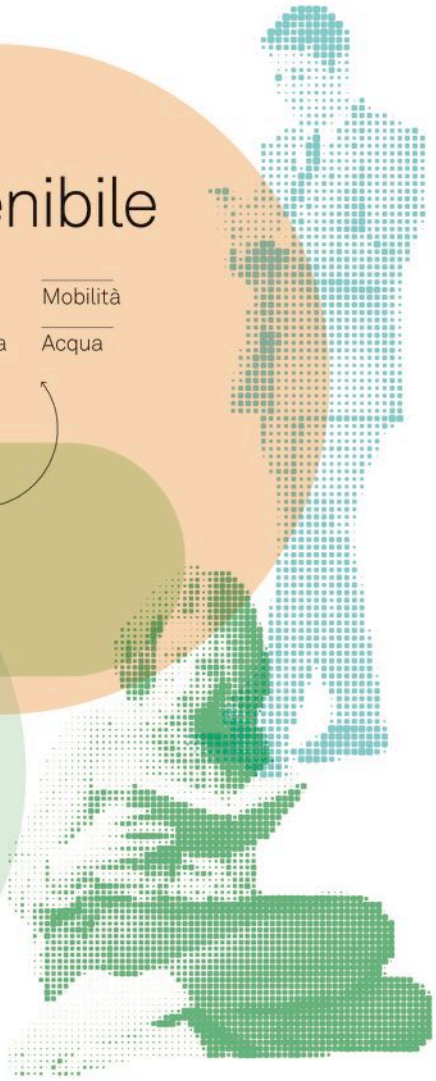
- Rifiuti
- Mobilità
- Logistica
- Acqua
- Energia

Amministrazione

La città circolare gestisce i processi con i cittadini e non per i cittadini, in una logica di costante interazione.

Inclusiva
Social

- Accoglienza e inclusione
- Storia e identità
- Sicurezza
- Spazi pubblici



Tre paradigmi della società

Colophon

Questo foglio esemplificativo è stato elaborato all'interno del Laboratorio

Politico della Fondazione Francesco Fabbri, coordinato da Roberto Masiero.

Autori:
Aldo Bonomi
Federico Della Puppa
Roberto Masiero

Con il contributo scientifico di:
Aaster
Theoremia

Progetto grafico:
Metodo studio.

Fondazione Francesco Fabbri Onlus

Sede legale
Villa Brandolini,
Piazza Libertà 7,
31053, Pieve di Soligo, TV

Sede operativa
Casa Fabbri,
Via Francesco Fabbri 1/B,
30153, Pieve di Soligo, TV

M 334 9677948
F 0438 694711
info@fondazione
francescofabbri.it
fondazionefrancescofabbri.it

http://twitter.com/FFFabbri
www.facebook.com/
FondazioneFrancescoFabbri

creative commons

Fondazione Francesco Fabbri
Politiche e Arti per i Territori

Società verticale

È la società imperniata sul motore progressista della dinamica tra capitale e lavoro a forte regolazione statuale. La grande fabbrica fordista, organizzata secondo i principi tayloristici, è l'epicentro della dinamica capitalistica intorno al quale si snodano le articolazioni della rappresentanza sociale, economica e politica. Lo Stato produce cittadinanza attraverso l'estensione progressiva dei diritti politici e sociali e gli investimenti infrastrutturali. Dal punto di vista territoriale la fabbrica fordista si sviluppa nei grandi poli urbani industriali secondo precise politiche di insediamento a capitale privato o pubblico. L'architettura istituzionale a piramide discende dallo Stato centrale alla periferia delle municipalità. L'inclusione e la mobilità sociale sono promossi attraverso il welfare state. L'ordinamento della società si muove dall'alto al basso, dal centro alla periferia, attraverso una fitta ramificazione di poteri intermedi e locali deputati alla realizzazione delle logiche del centro.

1. Fordismo:
Capitale – lavoro – Stato che ridistribuisce.

Società orizzontale

È la società che pone al centro il territorio come principio organizzativo della produzione, dell'inclusione e della mobilità sociale. La reticolarità dell'impresa diffusa nata dal sommerso, si impone con i distretti industriali, evolve in piattaforme produttive ed è l'epicentro della prima fase della globalizzazione in cui le economie locali organizzate affrontano la sfida dell'economia dei flussi globali. Il contado industrializzato prende il sopravvento sulla dimensione urbano – industriale, costituendosi come luogo privilegiato dell'autoimprenditorialità e come dispositivo di inclusione e mobilità sociale. L'assetto istituzionale statuale tende a devolvere potere legislativo ed esecutivo alle istituzioni periferiche, e numerose funzioni a controllo statuale vengono progressivamente privatizzate formando il nocciolo duro dei capitalisti delle reti, per un ampio terzo settore cui è delegata una parte importante del welfare. In questo quadro di erosione dei diritti sociali l'autoimprenditività diffusa diventa il vero principio di inclusione secondo uno schema in/out.

2. Capitalismo molecolare:
Territorio – corpi intermedi – Stato che regola.

Società circolare

È la società contemporanea attraversata da crisi capitalistiche ricorrenti, instabilità geopolitica diffusa, concentrazione del principio ordinatorio dei flussi a livello globale, disintermediazione della microfisica dei poteri di bilanciamento e trasmissione politica, crisi profonda del principio della rappresentanza a tutti i livelli. Finanziarizzazione e digitalizzazione della vita quotidiana sono i principali motori globali della circolarità ricorsiva che include con il debito, con le migrazioni, rendendo disponibili merci e servizi a basso costo in cambio della valorizzazione della socialità umana; capitalizza la condivisione dei doveri, riduce e sposta la sfera dei diritti sociali nel campo della regolazione dell'ordine pubblico (reddito di cittadinanza che diventa reddito minimo di circolarità). In questo quadro lo Stato non è più il soggetto centrale della società verticale, è sempre meno il regolatore della società orizzontale, è sempre più il mediatore (forte o debole a seconda della tradizione statuale nazionale) della potenza dei flussi sulla vita nuda della persone.

3. Sharing economy:
Flussi – corpo biopolitico – Stato che media.

Una strategia di Cyber Security per mitigare i rischi in ambienti critici e complessi: il caso degli aeroporti

Samuele Foni

Luca Ronchini

Autori: Samuele Foni e Luca Ronchini*

Abstract

Gli aeroporti sono sistemi critici e complessi che rappresentano un argomento di studio esemplare per stabilire un framework di cyber security flessibile e riutilizzabile per la mitigazione dei rischi legati agli aspetti di sicurezza informatica. Un sistema complesso è costituito da elementi interconnessi (agenti), ciascuno dei quali è in grado di adattare il proprio comportamento nel tempo per rispondere tanto ai cambiamenti ambientali che d'interazione reciproca [3]. All'interno di tali infrastrutture, il concetto di sicurezza assoluta non esiste, perché non è possibile proteggere l'intero sistema da qualunque tipo minaccia che potrebbe emergere, soprattutto per quanto concerne i rischi legati all'errore umano e alle circostanze di deterioramento (hardware e software) degli apparati IT. Tuttavia, l'uso corretto delle best practices di sicurezza informatica, l'adozione di un approccio investigativo top-down periodico e stratificato, la revisione continua dei processi operativi, l'impiego di un opportuno piano di cyber resilience e la formazione del personale attraverso corsi di formazione, aventi l'obiettivo di accrescere la consapevolezza dei dipendenti sulle questioni di sicurezza, possono bloccare il fenomeno, limitando la probabilità di innescare eventi che potrebbero causare danni a persone, strutture e risorse, impedendo alle compagnie aeroportuali di subire potenziali perdite economiche o danni d'immagine. In questo caso, l'unica soluzione praticabile è quella di stabilire una procedura ciclica di miglioramento della sicurezza informatica, che riproduca un adeguato compromesso in termini di protezione ed usabilità, avente l'obiettivo di unire le nuove procedure alla comune prassi quotidiana, evitando qualunque tipo d'impatto sulla missione aziendale.

In questa analisi verrà valutata la sicurezza dell'aeroporto utilizzando una visione emergente, ispirata ai paradigmi della *stigmergia* e dell'intelligenza sciame, al fine di stabilire un controllo capillare dei sistemi complessi dotati di una natura caotica, interconnessa, sociotecnica e fortemente dinamica, sia dal punto di vista fisico che operativo. Scopo della ricerca è la mitigazione del rischio legato alle debolezze aeroportuali, sfruttando un approccio analitico dei sistemi complessi in virtù di un miglioramento continuo della cyber resilience.

BIO

Samuele Foni è un Cyber Security System Engineer presso Thales Group, e lavora nelle attività di ricerca collegate al progetto SESAR2020.
samuele.foni@thalesgroup.com

Luca Ronchini è un Security Expert presso Thales Group, con una solida esperienza in materia di infrastrutture IT e gestione di architetture complesse, reti e sicurezza delle reti.
luca.ronchini@thalsegroup.com

Introduzione

Un *Sistema Complesso* è un sistema la cui evoluzione non può essere determinata a partire dall'analisi di tutte le componenti e di tutti i parametri d'ingresso che ne dovrebbero condizionare il comportamento. Viceversa, un *Sistema Critico* è un sistema che deve operare con un alto profilo di affidabilità, dal momento che un suo fallimento potrebbe provocare seri danni a cose, ambienti e persone, il più delle volte di natura irreparabile. Inoltre, è opportuno considerare un'altra categoria di sistema, quella dei *Sistemi Complicati*. Questi ultimi possono essere descritti

formalmente come un insieme di dispositivi, protocolli e procedure che sono difficili da configurare, ma che forniscono dei parametri d'uscita assolutamente predicibili. Gli aeroporti sono dei sistemi complessi, critici e complicati. Per questo motivo, essi rappresentano un eccellente banco di prova per affrontare lo sviluppo di un *Framework di Cyber Security* che funzioni efficacemente in tutti questi contesti. Inoltre, da parte della comunità di *Air Traffic Management* (ATM), sta nascendo un forte interesse sulle tematiche di cyber security, come dimostrano i vari contesti di ricerca attiva che fanno parte degli obiettivi del progetto di sviluppo SESAR2020. Specialmente quelli che fanno leva sull'indagine del numero crescente d'interconnessioni che devono essere stabilite tra i sistemi a bordo degli aeromobili e quelli dislocati a terra, stando a quanto previsto dagli standard di crescita degli aeroporti di nuova generazione [1].

All'interno di questo paper, viene dapprima fornita una breve spiegazione di quali siano i limiti degli approcci tradizionali alla cyber security, quando si ha a che fare con un sistema di natura complessa. Nella terza sezione viene affrontata l'analisi di un framework prototipale di cyber security, utilizzabile per la messa in sicurezza dei sistemi critici e complicati. Nella quarta sezione è riportato un esempio teorico d'integrazione delle tecniche d'intelligenza artificiale al framework precedentemente descritto, con l'obiettivo di renderlo adatto alla messa in sicurezza dei sistemi complessi. Infine, le conclusioni sono riportate all'interno della sezione V.

I limiti degli approcci tradizionali di cyber security nei contesti complessi

Gli attacchi informatici sono come le infezioni patologiche e, come tali, sono spesso frutto di una combinazione di circostanze, più che il risultato dello sfruttamento di una vulnerabilità isolata. In altre parole, è la "totalità" delle azioni e delle circostanze sfruttate dagli attaccanti a causare il danno [2]. Il problema è che le strategie tradizionali d'indagine, come quelle che si avvalgono del principio del *divide et impera*, sono fortemente incentrate sulla causalità degli eventi, ma un sistema complesso non può essere studiato semplicemente analizzando le parti che lo compongono [6]. Ne è una conferma il fatto che, nonostante l'impiego di sofisticati sistemi di cyber security, perfino stratificati, gli attacchi informatici continuino, comunque, a verificarsi. Questo perché l'uso delle tecniche tradizionali d'indagine induce, inevitabilmente, a cadere vittima di un paradosso (come dimostrato da Turing all'interno del suo *problema dell'indecidibilità dell'arresto*): non è possibile costruire una macchina che possa testarne un'altra in tutte le sue evoluzioni, ma per trovare tutti i malfunzionamenti e le vulnerabilità custoditi all'interno di essa, è necessario testarne il sistema completamente. Questa è la ragione per cui è opportuno investire sull'uso di un approccio olistico, per poter sperare di riuscire a portare avanti con successo una valutazione del comportamento emergente dei sistemi complessi.

Come costruire un framework per la mitigazione dei rischi in ambienti critici e complicati

Malgrado i limiti evidenziati in precedenza, le tecniche tradizionali di cyber security costituiscono il fulcro della messa in sicurezza di un sistema e, in quanto tali, non possono e non devono essere omesse. Di fatto, un uso appropriato di queste tecniche è di per sé sufficiente a garantire un elevato profilo di protezione delle infrastrutture critiche e complicate. In particolare, se l'insieme delle best practices di cyber security entra a far parte dello sviluppo costante di un'infrastruttura, per mezzo dell'adozione di un framework flessibile, dinamico e ben strutturato, è possibile ridurre drasticamente sia il fattore di rischio che il numero di vettori sfruttabili da parte di una minaccia cyber.

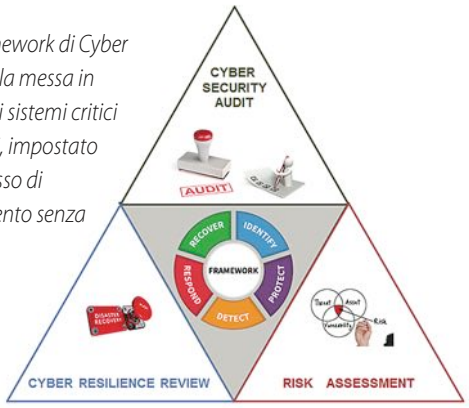


Fig. 1. *Framework di Cyber Security per la messa in sicurezza dei sistemi critici e complicati, impostato come processo di aggiornamento senza fine.*

Il lavoro di ricerca relativo alla messa in sicurezza dei sistemi critici aeroportuali, effettuato per il progetto SESAR2020, è stato particolarmente fruttuoso in tale contesto, maturando lo sviluppo di un framework di cyber security atto a gestire in continuità temporale la messa in sicurezza dei sistemi critici e complicati, sfruttando un approccio d'analisi di tipo Top-Down. Il framework sfrutta i concetti consolidati dai principali standard di cyber security per intervenire attivamente nell'identificazione, nella protezione, nella scoperta e nella reazione di tutte le minacce legate alla sfera cyber, oltre che nel ripristino delle funzioni operative. La costruzione e l'aggiornamento di queste procedure, però, è frutto di periodiche attività d'indagine, rappresentate in Fig. 1 da tre blocchi logici principali: *Cyber Security Audit, Risk Assessment e Cyber Resilience Review*. Il livello di dettaglio a cui intervengono queste attività cresce via via che si scende dall'alto verso il basso, seguendo una struttura piramidale. Svolgere periodicamente queste tre attività significa migliorare lo stato e le capacità del framework sotto ogni aspetto, fornendogli nuovi scenari da considerare, nuove contromisure da adottare, nuove minacce da valutare e così via, andando a stabilire un progresso continuo calato sulle necessità dell'infrastruttura.

a. Cyber Security Audit

Partendo da una visione di altissimo livello, nella quale si è a conoscenza esclusivamente del sistema nel suo insieme, senza essere al corrente dei dettagli che realizzano le sue parti, viene dapprima effettuata una lunga serie di questionari, tanto agli operatori che ai manager dell'infrastruttura, con l'obiettivo di adempiere alle seguenti finalità:

- valutare se le best practices di cyber security sono state applicate in maniera opportuna;
- enumerare i sotto-sistemi che costituiscono l'infrastruttura;
- identificare i processi operativi impiegati;
- aumentare il livello di consapevolezza relativo ai rischi legati alla cyber security a tutto il personale coinvolto;
- elencare i punti d'accesso al sistema sia a livello fisico che digitale.

In secondo luogo, occorre effettuare una prima analisi dei risultati ottenuti, per poi procedere in un'indagine sempre più dettagliata, volta ad identificare, da un lato, gli *Asset* principali del sistema, dall'altro, gli apparati di controllo degli accessi e

quelli di difesa perimetrale. Queste informazioni andranno a costituire i parametri di input delle azioni successive, rispettivamente di Risk Assessment e di Cyber Resilience Review; mentre gli scenari emersi dall'output dell'attività di Cyber Security Audit entrerano a far parte del framework.

b. Risk Assessment

L'obiettivo di questa attività è storicamente quello di effettuare una valutazione dei rischi. Si procede prendendo in ingresso la lista degli asset primari individuati precedentemente e se ne fornisce una misura di priorità. Successivamente si associa ogni asset ai sotto-sistemi e ai dispositivi che esercitano una certa influenza su di esso. Scendendo ancora di più nel dettaglio, si identificano le vulnerabilità legate a tutti questi apparati di supporto, tramite delle attività di *Vulnerability Assessment* e di *Penetration Testing*. Infine, si effettua una valutazione dei rischi (associati tanto alle vulnerabilità che alle minacce individuate), gli si fornisce una misura di probabilità e se ne determina il grado di accettabilità. Da questa attività emergeranno delle operazioni di patch management, di code review e di hardening, che andranno a rafforzare le misure di sicurezza dell'intero framework di cyber security.

c. Cyber Resilience Review

Partendo dall'analisi dei file di configurazione degli apparati d'accesso e di difesa perimetrale, occorre verificare il livello di resistenza e di robustezza dell'infrastruttura. Si procede effettuando un controllo approfondito delle contromisure in campo, oltre che dei sistemi di detection, di allarme, di notifica e di prevenzione. Per poi passare alla verifica del piano di disaster recovery impiegato, cercando soprattutto di valutarne l'efficienza, l'efficacia ed il grado di ridondanza. Infine, occorre effettuare un controllo capillare dei sistemi di risposta, esaminandone la flessibilità ed i tempi di reazione. Un'indagine di questo tipo deve rendere il sistema in grado di "imparare" dai propri errori, equipaggiando il framework di nuove contromisure, di nuovi processi operativi e di nuove tecniche di risposta che ne profilino l'evoluzione.

Come incrementare l'affidabilità del sistema, tramite l'inclusione di un approccio basato sulla complessità alla strategia di cyber security descritta in precednza

L'approccio descritto in precedenza è perfettamente in grado di gestire un sistema critico e complicato, dal momento che consente di minimizzare drasticamente:

- l'errore umano o procedurale;
- i vettori di rischio legati all'infrastruttura;
- il numero degli attacchi portati avanti con successo.

Il problema è che questo scenario non basta a gestire al meglio un sistema complesso; e che, allo stato attuale, non esistono tecniche abbastanza sofisticate da consentirne un controllo automatico efficiente. È in questo contesto che si fa strada l'idea di introdurre delle tecniche d'intelligenza artificiale applicate alla cyber security, con l'obiettivo di ridurre

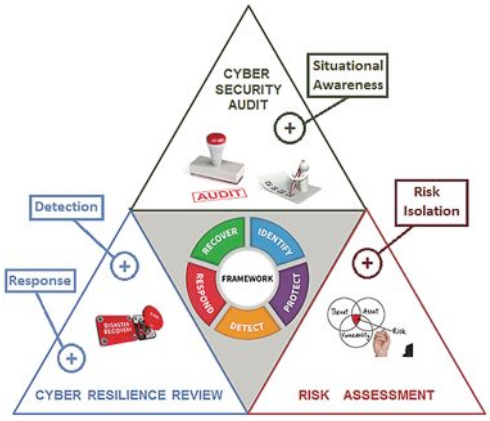


Fig. 2. *Framework di Cyber Security con l'aggiunta dei principali miglioramenti introdotti dall'adozione di un approccio orientato all'applicazione delle tecniche d'intelligenza artificiale per la messa in sicurezza dei sistemi complessi.*

ulteriormente l'eventualità che vengano portati avanti degli attacchi al sistema, non tanto perché sia essenziale proteggere un sistema complesso, ma perché questi sistemi sono critici e, in quanto tali, devono essere protetti con l'ausilio di qualunque mezzo a disposizione.

In letteratura, è possibile individuare alcuni esempi di applicazione dell'intelligenza artificiale alla cyber security, per lo più teorici, con lo scopo di apportare delle migliorie ad uno o più degli aspetti seguenti [5]:

1. Detection;
2. Situational Awareness;
3. Risk Isolation;
4. Response.

Prendendo in considerazione il framework presentato in Fig. 1, si potrebbe pensare di equipaggiarlo di tutte e quattro queste caratteristiche, ottenendo così lo schema riportato in Fig. 2. A colpo d'occhio, è evidente che, ben due, degli improvement più immediati derivanti dall'intelligenza artificiale applicata alla cyber security, insistono nell'attività di Cyber Resilience Review. Questo risultato non è frutto del caso: infatti, la Cyber Resilience rappresenta il motore versatile ed adattivo dell'intera infrastruttura e, come tale, è essa stessa un sistema complesso. Migliorare l'attività di Cyber Resilience Review, sfruttando un approccio orientato alla gestione dei sistemi complessi, è la chiave per ottimizzare il processo di mitigazione delle minacce informatiche. Si pensi, ad esempio, ai sistemi biologici, che rappresentano un ottimo esempio di sistema complesso, il cui elemento di forza è caratterizzato dalla loro robustezza ai disturbi ed ai cambiamenti. Se si astrae tale concetto, questo non è che un altro modo di definire la Cyber Resilience.

L'introduzione della *Swarm Intelligence* in ambito cyber è un primo esempio di integrazione delle tecniche di intelligenza artificiale nel campo dell'indagine adattiva del comportamento evolutivo di un sistema complesso. In questo contesto, una strategia percorribile è quella di utilizzare un approccio basato sugli agenti a più livelli, progettato per adattarsi rapidamente ed autonomamente alla gestione delle anomalie che vengono rilevate, sfruttando le caratteristiche di semi-razionalizzazione e di self-learning degli agenti, disposti in un arrangiamento gerarchico, per interpretare e correlare gli eventi su base logica, al fine di migliorare la comunicazione, l'interazione e l'intervento tra l'operatore umano ed il sistema. Lo scopo della disposizione gerarchica è quello di dare all'uomo un singolo punto di influenza che gli consenta di abilitare, con un'azione semplice, molteplici punti d'effetto [4].

a. Un modello di swarm intelligence multi-strato

Partendo dalle ultime considerazioni, un modello ben congeniato di questo tipo è teoricamente in grado di fornire un miglioramento immediato in termini di capacità gestionali del sistema nelle operazioni di detection, response, risk

isolation e situational awareness. La Fig. 3 riporta un esempio d'implementazione di un modello di analisi basato sulla swarm intelligence multi-strato, ispirato alla struttura gerarchica utilizzata dalle formiche. Si tratta di uno schema di alto livello, ma che fornisce una prima idea di realizzazione della piattaforma. Al livello più basso della gerarchia troviamo i *lavoratori,* ovvero i sistemi di elaborazione e di raccolta massiva dei dati, tra cui figurano i log analyzer, i sistemi IDS, le sonde cyber, gli script automatici che elaborano o forniscono dati, e così via. Questi lavoratori devono avere le seguenti caratteristiche: devono effettuare esclusivamente delle operazioni semplici, devono poter comunicare direttamente solo con gli agenti di livello superiore, devono essere autenticati e devono essere presenti in tutte le parti che compongono il sistema. La comuncazione tra lavoratori paritetici deve poter avvenire esclusivamente in maniera implicita, per effetto delle variazioni e delle anomalie che emergono a partire dall'osservazione dell'ambiente circostante, nel pieno rispetto dei principi della *stigmergia.*

Lo strato intermedio deve preoccuparsi di effettuare una scrematura dei dati che sono stati raccolti dai lavoratori, utilizzando dei motori intelligenti di analisi e di correlazione dati. Questo livello prevede una prima serie di scelte, che possono essere riassunte come segue: generazione di allarmi da passare al livello superiore per essere sottoposti ad un'ulteriore valutazione, gestione degli interventi diretti per bloccare in tempo reale gli attacchi in corso e filtraggio dei dati superflui. A questo livello possiamo trovare i SIEM di medio livello *(formiche maschio)*, che effettuano le operazioni di elaborazione e correlazione, ed i sistemi IPS e/o EDR *(formiche soldato)*, che si preoccupano di intervenire tempestivamente su una minaccia. Teoricamente, per rendere veramente efficiente l'attività di analisi e correlazione portata avanti a questo livello, tutti gli apparati di medio livello dovrebbero essere dotati di un motore di autoapprendimento.

Al vertice della gerarchia troviamo il SIEM di alto livello *(formica regina)*, dotato di un motore avanzato di analisi e correlazione dati, interamente basato sull'intelligenza artificiale, in grado di raccogliere gli allarmi che provengono dai vari SIEM di medio livello e di estrapolarne un'informazione chiara, esatta e georeferenziata da passare all'operatore umano. Compito di quest'ultimo sarà quello di effettuare l'ultimo livello di filtraggio che si tradurrà nell'applicazione di un intervento di alto profilo volto a protezione dell'infrastruttura e quindi della safety. Il fatto che all'operatore umano venga passata un'informazione e non un dato è essenziale per determinare il corretto funzionamento del modello.

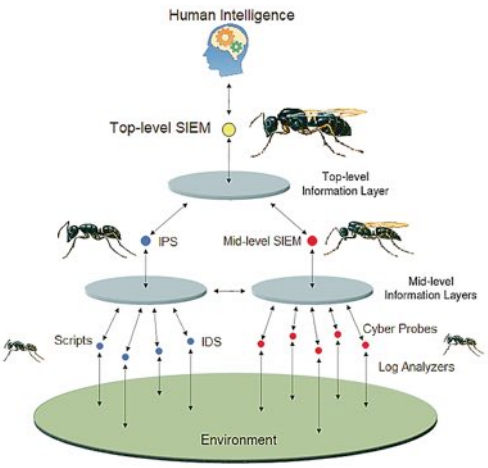


Fig. 3. *Modello teorico di un Framework di Cyber Security che fa uso della swarm intelligence multi-strato per migliorare le capacità di detection, response, situational awareness e risk isolation dell'intero sistema, ispirato alla struttura gerarchica delle formiche.*

Conclusioni

Lo scopo finale della costruzione e dell'adozione di un Framework di Cyber Security votato alla protezione dei sistemi complessi, critici e complicati è quello di salvare la vita delle persone. L'impatto di un attacco informatico su un sistema critico può essere letteralmente devastante, il più delle volte completamente inammissibile, per questo motivo è importante investire nella cyber security e nella ricerca di strategie sempre più efficienti che consentano alle compagnie di identificare e valutare una minaccia in tempo reale.

Nonostante non esista una soluzione definitiva a tutte le minacce informatiche che possono mettere a repentaglio il normale funzionamento di questi sitemi, è necessario ridurre il più possibile il livello di indeterminatezza legato allla manifestazione di un'anomalia, automatizzando al massimo le operazioni di detection e di correlazione degli eventi assoggettabili ad un attacco, con l'obiettivo di portare all'attenzione dell'operatore umano un risultato semplice ed immediato. Formalmente, l'introduzione delle tecniche d'intelligenza artificiale nelle strategie d'analisi della cyber security ha lo scopo di sintetizzare le informazioni di allarme, che pervengono dai vari dispositivi che compongono il sistema, al fine di consentire all'operatore umano di intervenire prontamente a salvaguardia della sicurezza delle persone e del sistema.

Abbreviazioni

- EDR - Endpoint Detection and Response
- IDS - Intrusion Detection System
- IPS - Intrusion Prevention System
- SIEM - Security Information and Event Management

Bibliografia

[1] Delain, O., Ruhlmann, O., Vautier, E., Johnson, C., Shreeve, M., Sirko, P., Prozserin, V. (2016). *Cyber-security application for SESAR OFA 05.01.01-Final Report.* OFA 05.01.01-D3

[2] Gandhi, Gagan. (2014). *Complexity theory in Cyber Security.* University of Warwick.

[3] Holland, J. H. (1995). *Hidden order: How adaptation builds complexity*. Helix Books.

[4] J. N. Haack, G. A. Fink, W. M. Maiden, A. D. McKinnon, S. J. Templeton and E. W. Fulp, *Ant-Based Cyber Security,* 2011 Eighth International Conference on Information Technology: New Generations, Las Vegas, NV, 2011, pp. 918-926.

[5] Oltsik, J., Poller, J. (2017). *Automation and Analytics versus the Chaos of Cybersecurity Operations.* ESG Research Insights Paper.

[6] S. A. McLeod (2008). *Reductionism and Holism.* ■

* Questo lavoro è stato supportato dall'attività di ricerca condotta da Thales Italia per il progetto SESAR2020. Nello specifico, SESAR2020 costituisce un programma di ricerca composto da svariati progetti, che mira a delineare quella che sarà la prossima ondata generazionale dei sistemi d'innovazione destinati alla gestione del traffico aereo in Europa. All'interno di questo contesto, Thales Italia è direttamente coinvolta nello sviluppo di un paio di progetti, uno dei quali è interamente dedicato alla cyber security.

Realtà industriali tra nuove tecnologie e preoccupazione per la sicurezza: tendenze, rischi e soluzioni dal mondo della cybersecurity

Autore: Morten Lehn
General Manager Italy di Kaspersky Lab

KASPERSKY lab

All'interno delle realtà industriali di tutto il mondo, fenomeni legati alla trasformazione digitale – come la convergenza tra il mondo dell'Information Technology (IT) e quello dell'Operational Technology (OT), la maggior connettività dell'OT alle reti esterne e il crescente numero di dispositivi IoT ad uso industriale (IIoT) – stanno contribuendo a migliorare l'efficienza dei processi e delle lavorazioni.

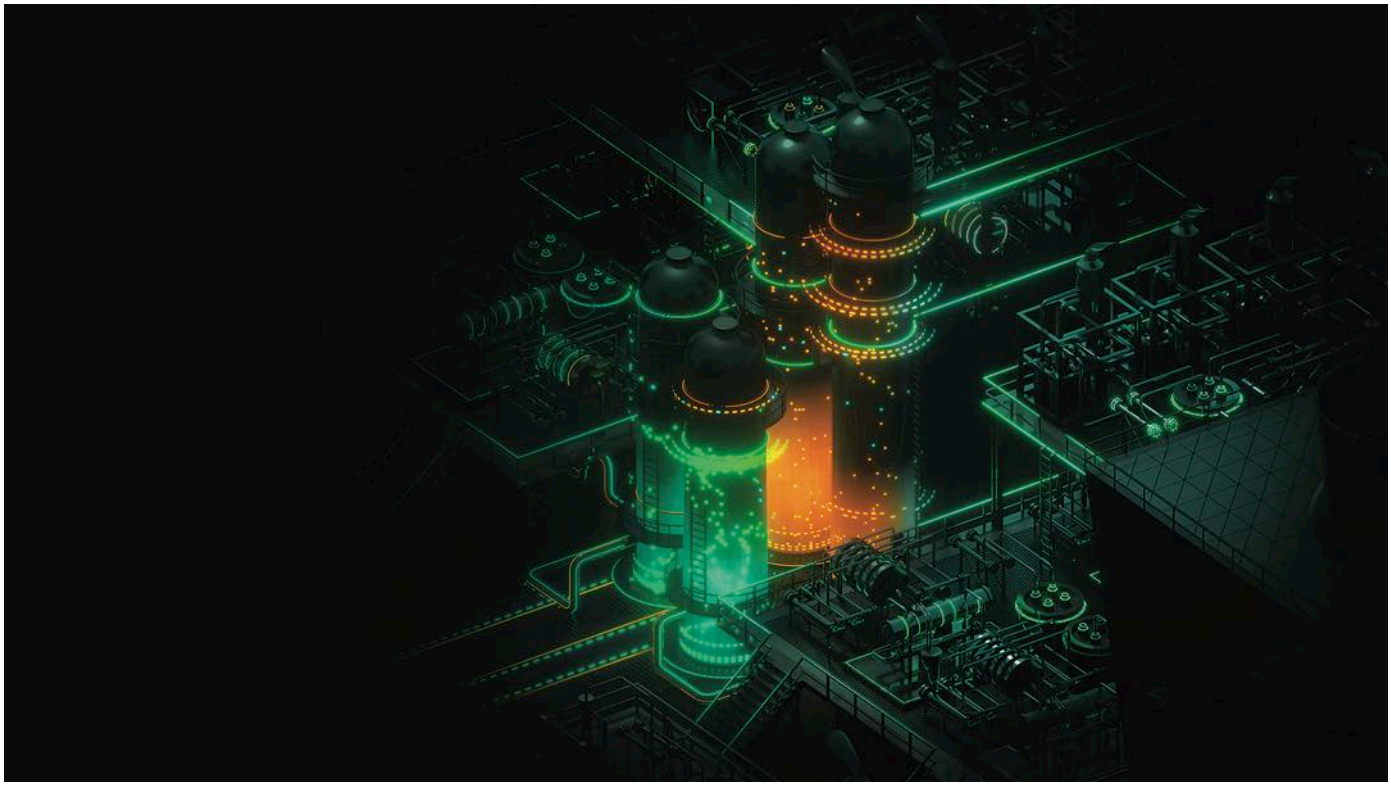
BIO

Norvegese di nascita, Morten Lehn a luglio 2014 è stato nominato General Manager Italy di Kaspersky Lab, diventando il punto di riferimento dell'azienda per il mercato italiano.
Prima di ricoprire questa carica è stato Sales Director sempre in Kaspersky Lab, occupandosi delle attività di tutto il sales team dell'azienda, per il segmento B2B Corporate ed Enterprise, B2C Consumer e per le vendite online.
Prima di approdare in Kaspersky Lab nel 2013, ha lavorato presso il distributore di informatica Bludis, in qualità di Sales Manager dal 2002 al 2009 e in seguito di Sales Director, rispondendo direttamente al CEO dell'azienda. In precedenza Lehn è stato Business Development Manager in Unified Messaging Systems AS, dove ha gestito la start up della filiale italiana dell'azienda, e Sales Manager in Euroline AS.

Tuttavia, questo tipo di tendenze portano con loro non solo vantaggi, ma anche rischi per quanto riguarda la sicurezza, moltiplicando i possibili punti di vulnerabilità. Grazie alle maggiori possibilità di azione offerte dalle nuove tecnologie, gli attacchi si fanno sempre più frequenti e sempre più sofisticati.

Dall'analisi fatta dal nostro Industrial Control Systems Cyber Emergency Response Team (ICS Cert), il progetto globale lanciato nel 2016 con l'obiettivo di coordinare gli sforzi dei fornitori di sistemi di automazione, i proprietari di infrastrutture industriali, gli operatori e i ricercatori nell'ambito della sicurezza nella protezione delle industrie dai cyberattacchi, è emerso il quadro delle aziende più colpite da minacce informatiche nella seconda metà dello scorso anno. Le aziende del settore dell'energia sono state le più esposte: le soluzioni Kaspersky Lab a protezione dei loro ICS hanno rilevato almeno un tentativo di attacco malware all'anno nel 38,7% dei casi. In un'ipotetica classifica di settori più colpiti, al secondo posto troviamo quello dei network di engineering e integrazione ICS (con il 35,3%). Per altri ambiti di applicazione industriale la media è stata tra il 26 e il 30%.

La cybersicurezza negli impianti industriali è un problema di grande rilievo, perchè può portare a conseguenze molto serie e anche comportare perdite economiche ingenti in caso di attacchi ai processi di lavorazione e sviluppo.



Questi attacchi sono fonte di notevole preoccupazione, proprio perché ormai è chiaro che potrebbero portare a conseguenze catastrofiche, che vanno dai possibili danni ai prodotti alla perdita della fiducia da parte dei clienti e di opportunità commerciali, fino a problematiche a livello ambientale e cali nella produzione in uno o più stabilimenti. Un singolo cyberattacco può danneggiare i processi industriali e perfino minacciare la continuità operativa; se un incidente non viene identificato entro una settimana, il danno economico per l'impresa può arrivare a 1,2 milioni di dollari in media (un dato che proviene dal nostro report *"New Threats, New Mindset: Being Risk Ready in a World of Complex Attacks"*).

Secondo l'ICS CERT di Kaspersky Lab nella seconda metà del 2017 ben il 37,8% dei computer (ICS) in tutto il mondo hanno subito delle cyberminacce. Tra le organizzazioni che hanno subito almeno un incidente informatico al proprio sistema di controllo industriale negli ultimi 12 mesi, inoltre, il 20% afferma che il danno economico alla propria attività è cresciuto, fornendo un ulteriore incentivo per gli investimenti in migliori sistemi di cybersecurity.

Per tutti questi motivi le organizzazioni industriali si sentono sempre più a rischio: secondo un sondaggio più recente – dal titolo *"State of Industrial Cybersecurity 2018"*, che ha visto la partecipazione di 320 figure con potere decisionale nel campo della sicurezza informatica OT/ICS in realtà industriali di tutto il mondo – oltre i tre quarti (il 77%) delle aziende ritiene che la propria organizzazione possa diventare obiettivo di un incidente di sicurezza informatica diretto proprio alle reti del controllo industriale.

Malgrado la consapevolezza in aumento e gli investimenti per la sicurezza IT avanzata che stanno crescendo, quasi i due terzi (64%) delle aziende interpellate dichiarano di aver subito almeno un attacco tramite malware o tramite virus tradizionali negli ultimi 12 mesi sul proprio ICS.

Il 30% delle aziende dice di essere stato colpito da un attacco ransomware e un quarto (27%) di aver subito una violazione del proprio sistema di controllo industriale a causa di errori e cattive azioni da parte dei propri dipendenti. Gli attacchi mirati che hanno colpito il settore nel 2018 interessano solo il 16% (in calo rispetto al 36% registrato nel 2017).

Le aziende che si affidano agli ICS, quindi, continuano ad essere vittime di minacce convenzionali, inclusi malware e ransomware, così come di attacchi mirati. E l'attacco da parte di un ransomware, in particolare, può causare problemi di vasta portata ai sistemi critici, come dimostrato da numerosi incidenti (specialmente WannaCry e exPetr infection) che hanno colpito i sistemi ICS/SCADA nel 2017. Tra i trend dello scorso anno, i nostri ricercatori hanno scoperto anche un aumento degli attacchi di *mining* sugli ICS, dopo lo sviluppo del mercato delle criptovalute e dei *miner* in generale.

Comportando un significativo carico sui computer, agendo in modo negativo sulle operazioni dei componenti ICS dell'azienda e compromettendo così la loro stabilità, questo tipo di attacco può costituire una pericolosa minaccia per le industrie.

In questo quadro complesso, tra minacce reali e percezioni variabili, sembra che le organizzazioni stiano affrontando la questione della sicurezza informatica all'interno delle loro realtà e nelle loro reti in modo differenziato e con vari livelli di consapevolezza, tra un'idea del rischio che a volte sembra distante dalla realtà del panorama attuale delle minacce e approcci talvolta diversi tra mondo IT e OT. I nostri studi mostrano che le industrie, anche se hanno ben presenti i possibili rischi

che si associano ad una maggiore digitalizzazione, non stanno mettendo in atto le giuste pratiche di sicurezza informatica per proteggere le loro reti operative.

Il margine per una miglior integrazione tra IT e OT a livello di cybersecurity esiste. Lo testimonia l'ammissione fatta dal 48% delle organizzazioni riguardo al fatto di non avere messe in atto misure ad hoc per la rilevazione o il monitoraggio di eventuali attacchi subiti da parte delle loro reti di controllo industriale.

L'introduzione dell'IoT nel mondo della produzione industriale e dei sistemi basati su cloud, inoltre, ha portato il settore della sicurezza a confrontarsi con problematiche ulteriori e rappresenta una nuova sfida per le imprese industriali. Per più della metà delle aziende coinvolte (54%), il possibile aumento del rischio determinato da connettività e integrazione di ecosistemi IoT sarà un importante problema per la sicurezza informatica nel prossimo anno, nonché per la messa in atto di misure per la loro gestione. Con le aziende che investono sempre più in tecnologie smart e nell'automazione, con l'adozione di un approccio industriale 4.0, la tendenza ad una maggiore connettività e all'IoT può solo crescere. In effetti, quando si parla di implementazione del cloud, scopriamo che il 15% delle organizzazioni industriali utilizza già soluzioni cloud per i propri sistemi di controllo SCADA e che un ulteriore 25% sta pensando di implementarle nei prossimi 12 mesi. Questo quadro attuale porta con sé una forte spinta all'uso del cloud per la gestione ad alto livello delle infrastrutture critiche.

Molto si fa per la sicurezza in ambito IT, anche se in alcuni casi si continua a fare affidamento su modelli che si basano su convinzioni antiquate, come quelle che vedono nell'isolamento dei sistemi tramite *air gap* o nell'applicazione del principio della "Sicurezza tramite segretezza", traduzione dell'inglese "Security through Obscurity", la soluzione a qualunque tipo di situazione critica.

In questo panorama così sfaccettato, e anche così preoccupante, è, invece, fondamentale che le possibili misure di cybersecurity siano costantemente al passo con le novità tecnologiche: solo in questo modo si può garantire alle organizzazioni coinvolte il fatto che i possibili benefici andranno oltre i rischi. Le aziende devono occuparsi con maggior serietà dei programmi di risposta agli incidenti ICS, per evitare il rischio di gravi danni operativi, economici e reputazionali. Solo sviluppando uno specifico programma "incident response" e utilizzando soluzioni di cybersecurity dedicate per gestire la complessa natura degli ecosistemi industriali connessi e distribuiti, le aziende potranno tenere al sicuro i servizi, i prodotti, i clienti e il loro ambiente produttivo.

Uno dei casi più recenti di aziende che hanno deciso di affrontare in modo strutturale e corretto il discorso della sicurezza è quello della Pavlodar Oil Chemistry Refinery (POCR LLP), una delle maggiori società di raffinazione e produzione di petrolio del Kazakistan, che utilizza attrezzature avanzate e tecnologie di automazione per i propri processi industriali.

Per evitare attacchi, il dipartimento IT della raffineria ha avviato un progetto per migliorare la propria sicurezza informatica e le misure tecnologiche dei suoi processi industriali. Dopo aver considerato diverse opzioni, la Pavlodar ha scelto come piattaforma Kaspersky Industrial Cyber Security.

L'implementazione della soluzione in grado di garantire la sicurezza dei computer industriali e dei server SCADA, ma anche di fornire uno strumento per controllare i parametri fondamentali dei processi industriali senza avere alcun impatto su di loro e senza richiedere modifiche, così come la formazione dei dipendenti, sono stati passi fondamentali nella difesa dalle minacce informatiche.

Un altro caso interessante è quello di Plzeňský Prazdroj, la nota azienda produttrice di birra, conosciuta per la produzione della Pilsner Urquell e per aver dato origine ad una tipologia di birra che ora corrisponde a più dei due terzi della birra prodotta oggi nel mondo. L'azienda si è rivolta a Kaspersky Lab per rendere più solido il proprio sistema di cybersicurezza a livello industriale e per migliorare la resistenza agli attacchi informatici delle linee di produzione e delle tecnologie operative, identificando possibili vettori di attacco e mettendo in sicurezza eventuali falle nella sua complessa infrastruttura IT.

In questo caso i nostri esperti hanno avviato un assessment completo a livello di cybersecurity, una valutazione da remoto, minimamente invasiva e on-premise, che ha avuto inizio con un audit dell'Infrastruttura e con lo sviluppo di un modello di simulazione di minaccia su 2 birrifici e 8 linee di imbottigliamento dello stabilimento.

Dopo l'esame della rete aziendale connessa alla zona industriale, dei software SCADA e delle connessioni esterne prive di controllo da e verso il settore della produzione, è stato possibile mettere a disposizione un elenco delle vulnerabilità scoperte, delle vulnerabilità 0-day, i dettagli su possibili vettori di attacco e alcuni consigli da mettere in atto.

In questo modo il team per la sicurezza IT di Plzeňský Prazdroj ha scongiurato le disastrose conseguenze di un potenziale attacco che avrebbe potuto influire negativamente sulla sicurezza e l'affidabilità dei birrifici, oltre che sui risultati economici dell'azienda.

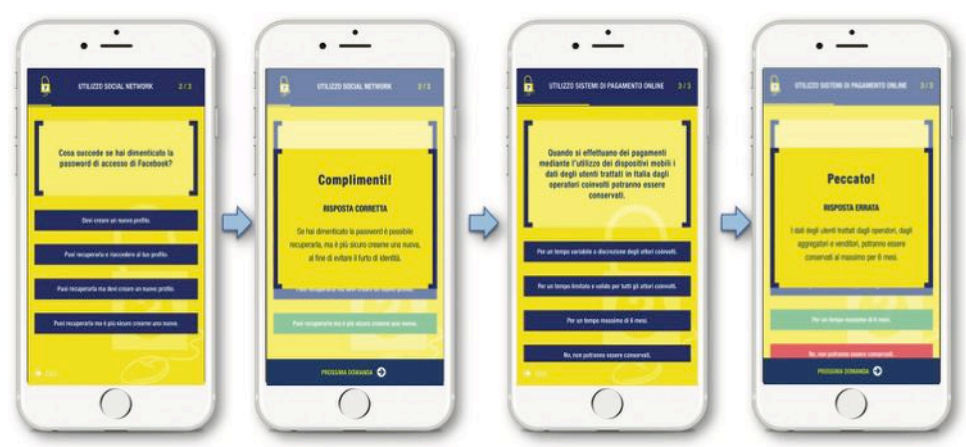
Questi due casi sono emblematici del tipo di approccio che le industrie dovrebbero avere in materia di cybersecurity. È sempre più importante implementare soluzioni di sicurezza complesse, altamente flessibili e configurate in conformità con i processi tecnologici di ciascuna organizzazione.

Le tecnologie e i servizi devono coprire le varie esigenze delle imprese industriali ed essere in grado di proteggere ogni livello, inclusi server SCADA, HMI, workstation di progettazione, PLC, connessioni di rete e postazioni di lavoro. Le soluzioni più adatte sono quelle in grado di coprire tutte le fasi del modello di sicurezza adattivo, dalla previsione di nuovi vettori di attacco all'uso di tecnologie specializzate per la prevenzione, il rilevamento e la risposta. ■

CyberSecQuiz

CyberSecQuiz è la piattaforma di Poste Italiane che testa il livello di conoscenza sulla sicurezza informatica e consente di aumentare e "alimentare" regolarmente la consapevolezza della sicurezza delle informazioni su internet attraverso dei test.
La piattaforma è stata ideata come uno strumento ludico che presenta all'utente un test quiz a risposta multipla, di difficoltà variabile, riguardante operazioni comunemente effettuate online, raggruppate nelle seguenti categorie: Internet, Posta Elettronica, Sistemi di Pagamento Online, Social Network e Smartphone.
CyberSecQuiz può essere utilizzato da qualunque dispositivo (mobile o fisso) ed è dedicato a studenti, lavoratori, aziende, associazioni e Istituzioni. Il quiz è composto da domande a risposta multipla selezionate in ordine casuale. Ogni domanda presenta 4 risposte di cui due sbagliate, una corretta ed una perfetta.

Un algoritmo intelligente assegna le domande in funzione delle risposte dell'utente, in base a tre livelli di difficoltà basso, intermedio e alto. Il grado di difficoltà delle domande varia in base alle risposte; aumenta se l'utente risponde perfettamente, rimane uguale se risponde correttamente, diminuisce in caso di errore.
Alla fine del quiz, l'utente viene inserito in un ranking generale in cui può comprendere il proprio livello di conoscenza sia comparandolo agli altri, sia comparandolo al quiz effettuato precedentemente.
L'utente può accedere a CyberSecQuiz in maniera del tutto anonima, oppure tramite login (Email e Password), o, in alternativa, compilando il form di registrazione per ottenere delle credenziali di accesso.
Cimentati con CyberSecQuiz di Poste Italiane per valutare quanto navighi sicuro perché la sicurezza online inizia dalla consapevolezza dei rischi!



Quanto ne sai di Sicurezza Informatica?
Fai un test su www.distrettocybersecurity.it/cybersecquiz/

I problemi di sicurezza delle smart grid: affrontare le minacce per trarre i benefici

Autore: Joseph Pindar

Vale la pena lottare per i benefici delle smart grid

Le *smart grid*, ovvero l'interconnessione "intelligente" fra una rete elettrica e una di comunicazione, permettono di creare una rete di distribuzione molto più efficiente, eliminando dall'equazione relativa alla produzione di energia la parte che si basa sulle ipotesi su quanta sarà effettivamente la richiesta. Infatti, le *smart grid* aumentano l'attendibilità raccogliendo i dati di consumo da dispositivi intelligenti, quali ad esempio gli *smart meter*, e fornendo i dati in tempo reale al sistema di produzione.

Usando questa informazione, il sistema di produzione è in grado di calcolare il punto di equilibrio, e bilanciare il carico sulla rete per evitare sovraccarichi e ottimizzare i tempi. I fornitori di energia potranno anche fornire ai clienti informazioni in tempo reale, come ad esempio il costo dell'energia in un dato momento, e creando nuovi modelli di costo basati sulla domanda.

Aiutando i consumatori ad usare meno energia, le *smart grid* possono contribuire alla riduzione delle emissioni di CO2 e altre sostanze inquinanti. Una *smart grid* fa sì che il sistema attivi le centrali solo quando necessario, perché i livelli di produzione sono basati sulla domanda in tempo reale. Inoltre, le *smart grid* aumentano l'integrazione di altre sorgenti di energie alternative, come quella solare e quella eolica, nell'ecosistema di generazione.

Le *smart grid* sono anche capaci di badare a se stesse, con sistemi che monitorano costantemente le condizioni complessive e che eseguono simulazioni per anticipare i problemi e intraprendere azioni risolutive nell'arco di secondi. Ad esempio, potrebbero attivare i contatori perché isolino un problema e bilancino la produzione su altri generatori, senza danneggiare fisicamente l'infrastruttura. Con questo tipo di strumenti, le *smart grid* sono anche in grado di prioritizzare le funzioni critiche da mantenere attive durante un disastro, come ad esempio l'illuminazione stradale e gli ospedali.

Il futuro delle *smart grid*

I benefici delle *smart grid* sono numerosi, e si potrebbe sostenere addirittura che saranno essenziali per la sostenibilità della società moderna. In effetti, secondo alcuni fornitori, il costo dell'energia elettrica aumenterà del 400% nei paesi occidentali che non attiveranno le *smart grid*.

Con una posta così alta in gioco, non dovrebbe sorprendere che lo sviluppo delle *smart grid* stia accelerando, con più di 13,3 milioni di *smart meter* installati e 2,7 miliardi di dollari investiti in progetti di *smart grid* negli Stati Uniti nel solo 2016.

Sfortunatamente, i problemi di sicurezza delle *smart grid* sono ugualmente numerosi, e questa forma di rete intelligente rischia di ampliare il panorama delle minacce.

Vista la centralità che rivestono, un fallimento sotto il profilo della sicurezza potrebbe mettere a repentaglio uno dei sistemi chiave della nostra società.

Tre questioni di sicurezza da risolvere

Possiamo classificare i potenziali cyber attacchi alle *smart grid* in tre categorie principali suddivise per obiettivo: attacchi contro i dispositivi (ad esempio, gli *smart meter*), attacchi contro le sorgenti (ad esempio i produttori di dispositivi) e attacchi alla comunicazioni fra sorgenti e dispositivi.

Attacchi contro i dispositivi

Per un potenziale hacker, un dispositivo è un obiettivo interessante per diverse ragioni. Primo, molti dispositivi hanno un valore intrinseco legato alla loro funzione. Uno *smart meter* raccoglie i dati di utilizzo dell'energia elettrica, che potrebbero essere d'interesse per qualcuno che sta cercando di danneggiarci. Un ladro, per esempio, potrebbe usare queste informazioni per stabilire quando il proprietario di casa è via, sulla base di come varia il consumo elettrico durante certe ore della giornata.

Alcune *smart grid* uniscono gli *smart meter* ad altri dispositivi domestici, per un controllo più granulare sull'uso dell'elettricità. Per esempio, il sistema modifica

leggermente le impostazioni del condizionatore per evitare un black-out. Sfortunatamente, lo stesso meccanismo può essere utilizzato dagli hacker per scopi molto meno nobili.

Infine, i dispositivi hanno un valore legato alla loro affidabilità. La *smart grid* si affida ai dati raccolti dallo *smart meter*, e alla loro accuratezza e veridicità. Gli hacker potrebbero modificare le impostazioni di uno *smart meter* per ridurre la bolletta o per nascondere attività illegali, ad esempio la produzione di droghe.

Attacchi contro le comunicazioni

Un comune metodo di attacco è quello attraverso il quale si monitorano e modificano i messaggi durante la loro trasmissione. La quantità e la criticità di dati che transitano da e per le *smart grid* rendono questi tipi di attacchi particolarmente pericolosi, perché i messaggi e i dati potrebbero essere intercettati, rubati, o manipolati mentre transitano. Queste minacce mettono a repentaglio l'affidabilità delle informazioni e dei dati che vengono trasmessi, e la fiducia complessiva che si può riporre nell'infrastruttura nel suo insieme.

Per esempio, le informazioni riguardo il consumo di energia che transitano dalla vostra abitazione o dal vostro ufficio verso il fornitore sono esposte a tutta una serie di minacce: per esempio, un hacker potrebbe tracciare il vostro consumo di elettricità per registrarne picchi e abbassamenti in modo da pianificare un attacco alla vostra proprietà, oppure potrebbe manipolare i dati trasmessi e modificare le informazioni.

Attacchi all'ecosistema

I principi di affidabilità per le Smart Grid

Un hacker preparato punterà al cuore della *smart grid*, perché un attacco riuscito a uno degli anelli della catena è in grado di fare il maggior danno possibile – o ottenere il maggior ritorno economico. Gli obiettivi possono essere produttori, fornitori, operatori di rete, impianti di produzione, e i servizi stessi.

Queste infrastrutture raccolgono e analizzano dati sensibili che gli hacker cercheranno di rubare. Sono gli obiettivi primari degli attacchi mirati a interrompere l'erogazione di un servizio, e saranno i primi target per malware e cyber-armi come Stuxnet.

Gli obiettivi di sicurezza delle *smart grid*

La sicurezza delle smart grid passa per alcuni obiettivi principali: disponibilità, integrità, confidenzialità e responsabilità *(accountability)*.

- **Disponibilità:** garantire l'accesso e l'uso delle informazioni in maniera puntuale e affidabile è un elemento centrale delle *smart grid*. I benefici delle *smart grid* non possono essere ottenuti se non è garantito un accesso effettivo, affidabile e in tempo reale ai dati. È anche estremamente importante come sono raccolti, collezionati e condivisi i dati, e occorrono soluzioni di sicurezza che perseguano questi obiettivi cercando di evitare conseguenze negative.
- **Integrità:** Le *smart grid* dipendono da dati accurati e affidabili. Per evitare frodi o altri attacchi più pericolosi, servono misure che garantiscano l'accuratezza delle informazioni e l'assenza di manipolazioni.
- **Confidenzialità:** Le *smart grid* generano grandi volumi di dati che devono essere raccolti, conservati e analizzati. Alcuni di questi dati contengono dettagli sensibili sui consumatori e i sistemi di produzione stessi. Devono essere implementate misure di protezione che impediscano la divulgazione non autorizzata di informazioni sensibili.
- **Responsabilità:** l'*accountability* è il principio secondo il quale un sistema o un utente dovrebbero essere responsabili delle proprie azioni. Questo significa che le interazioni fra un utente e un sistema sensibile dovrebbero essere registrate e ricondotte alla persona specifica. Questi log dovranno essere difficili da falsificare e dovranno essere adeguatamente protetti dalla compromissione dell'integrità.

L'ecosistema delle *smart grid* è intrinsecamente complesso, il che pone importanti questioni di sicurezza. I fornitori di software, *smart meter* e dispositivi, gli impianti di produzione, i mercati energetici, e le reti all'interno di cui operano devono essere tutti presi in considerazione quando si discute di sicurezza. E allo stesso modo, ogni anello della catena deve essere coinvolto in prima persona per il raggiungimento di tali, centrali, obiettivi. ■

BIO

Joseph Pindar è il Direttore della Strategia di Prodotto focalizzato sulla sicurezza e protezione dati. Lavora nella divisione del CTO, parte della business Unit *Gemalto Enterprise & Cybersecurity* (ex SafeNet).
Si dedica alla creazione e alla comunicazione della conoscenza situazionale rivolta a product manager e leader ingegneristici. Joe contribuisce altresì ad elaborare le linee guida e a definire le priorità nel processo di sviluppo per adeguarlo alle esigenze di mercato. Lavora inoltre con diverse Business Unit in Gemalto al fine di creare efficaci piani di mercato. Le tendenze e le tecnologie che Joe considera eccellenti in questo momento sono Blockchain, IoT, e sicurezza per il Cloud Foundry. Joe è anche membro fondatore della Trusted IoT Alliance, che lavora per BNY Mellon, Bosch, Cisco, Foxconn e altre sette start-up, usando la tecnologia Blockchain per garantire la sicurezza dell'Internet delle cose.
Prima di iniziare a lavorare presso Gemalto, Joe ha lavorato nel settore dello storage e per il governo del Regno Unito. Ha coperto diverse posizioni, tra le quali assistenza tecnica alla prevendita, consulenza sulla sicurezza e ricerca, architettura di rete e sviluppo ingegneristico. In qualità di membro del "blue team" Joe è stato premiato per la sua ricerca sull'allineamento dell'Information Assurance e la cyber Security con la strategia aziendale. Joe possiede un master in ingegneria dell'Università di Sheffield, una certificazione ISCS2 CISSP e contribuisce regolarmente all' ICS2 dirigendo webinar che vertono su argomenti riguardanti la Blockchain, l'IoT e le regolamentazioni emergenti.
Per ulteriori informazioni sulle smart grid https://blog.gemalto.com/security/2016/06/17/smart-grid-security-issues-addressingthreats-seize-benefits/

I cyber criminali non conoscono confini! Dakar, Senegal

Autore: Marco Essomba
CTO, iCyber-Security Group Ltd

A volte, la vita da imprenditore e fondatore di imprese può portarti in posti inattesi! Recentemente, ho trascorso una settimana a Dakar, in Senegal, Africa dell'ovest, per un progetto di formazione dei responsabili della sicurezza informatica dell'Ufficio Imposte, per la protezione dai cyber attacchi dell'infrastruttura di rete e degli applicativi online. Come in molti paesi, anche le aziende senegalesi stanno confrontandosi con la crescente minaccia mondiale rappresentata dal cyber crimine e con l'impellente necessità di proteggere i propri asset digitali per poter lavorare online in piena sicurezza.

L'inarrestabile crescita degli attacchi cyber

Abbiamo la tendenza a pensare al cyber crimine come a una minaccia occidentale. Ma in realtà, incombe anche nelle nazioni in via di sviluppo, dove il progresso è accelerato e la tecnologia tende a procedere a balzi. A partire dai cyber criminali, gli agenti governativi e gli hacktvisti che sferrano attacchi DDoS, per arrivare allo spionaggio industriale, la raccolta di informazioni e i tentativi di sottrarre informazioni sensibili, in tutto il mondo le aziende si stanno confrontando con la crescita del cyber crimine. Secondo Forbes, i costi del cyber crimine raggiungeranno i 2 trilioni entro il 2019.

Dakar – grande centro di scambio per l'Africa occidentale

La repubblica del Senegal, il paese africano più a ovest, si trova fra la Guinea-Bissau e la Mauritania e si affaccia sull'Atlantico del Nord, con una

costa e delle spiagge bellissime. Qui gli affari sono in pieno fermento: il Senegal è ritenuta una democrazia solida e pacifica, specie se paragonata a molte altre nazioni africane. Nel 2016, un referendum costituzionale ha introdotto un limite di 5 anni per il mandato presidenziale e un massimo di due mandati consecutivi.

La capitale del Senegal è Dakar, oggi uno dei maggiori centri di scambio dell'Africa occidentale. Per rinforzare questa posizione strategica, il Governo si sta impegnando in una enorme rivoluzione digitale guidata dai servizi online (e-services). Aziende e cittadini potranno a breve pagare le tasse online, da qualsiasi posto, qualsiasi device e in qualsiasi momento! Con l'esempio, il Senegal si pone alla guida della rivoluzione digitale africana.

BIO

Marco Essomba (Certified Application Delivery Networking and Cyber Security Expert)è un leader riconosciuto nel campo dell'industria. È il fondatore ed il CTO di iCyber-Security Group, una ditta novatrice di cyber security basata in UK, specializzata in soluzioni di digitale per le PMI, complete e competitive. La piattaforma di difesa di iCyber-Security (iCyber-Shield) offre una visibilità ed un controllo totale sull'insieme dell'infrastruttura di sicurezza, essendo quotata presso il London Digital Security Centre Market Place. Potete connettervi con Marco suTwitter (22K+ followers) su @marcoessomba oppure via LinkedIn: (10K+ followers) all'indirizzo: https://uk.linkedin.com/in/marcoessomba

E-confini senza conflitti

Una volta atterrati all'aeroporto internazionale Leopold Sedar Senghor, il processo di controllo passaporti è rapido e liscio. Lettori di impronte digitali, scanner di passaporti digitali e di bagagli accompagnano verso l'uscita dall'aeroporto. Il livello di sicurezza sembra molto alto.

Interagendo con gli abitanti del posto

Ho preso un taxi dall'aeroporto: molti taxi africani sono dipinti di giallo ed è facile distinguerli. Volevo provare l'esperienza del contrattare, abitudine tipica in Africa dove il prezzo è relativo e può essere sempre negoziato.

Il mio stile di negoziazione, improntato all'idea win-win, mi pone in posizione ottimale. Mi siedo davanti, per ottenere il più possibile dal tassista e fare buon uso del mio francese. In breve, ottengo uno sconto, e queste sono soddisfazioni!

Partiti con il piede giusto, e con il mio francese in grande spolvero, il tassista sente l'accento inglese e immediatamente cambia lingua. È desideroso di mostrare le sue abilità e io sono ben felice di farlo contento. Lo parla bene, fluidamente. "Come mai parli un così buon inglese?" chiedo. "Non l'ho studiato. L'ho imparato parlando con la gente che prendo qui all'aeroporto."

Il boom di Internet

Si percepisce la forte spinta che ha avuto la connessione internet qui. Sul telefono ho 4g. La connessione è molto veloce. I tempi di risposta sono trascurabili. Dovunque mi volti, le persone sono al telefono. Chattano, navigano sui social, mandano messaggi. È evidente che qui a Dakar la connessione non è un problema.

Difesa in profondità. Difesa per livelli.

Ritorniamo allo scopo del mio viaggio: formare i responsabili della sicurezza dell'Ufficio Imposte senegalese e aiutarli a pianificare, progettare e implementare un'infrastruttura sicura per accompagnare la trasformazione digitale.

Per rendere disponibili online i vari servizi governativi attraverso un portale web, è necessario rendere l'infrastruttura di rete e applicativa molto veloce, sicura e sempre disponibile. Per farlo, c'è bisogno di data center nazionali capaci di sostenere la richiesta crescente e mettere quindi aziende e cittadini in condizione di aggiornare le loro tasse online. Ovviamente, tutto questo comporta anche i rischi comunemente associati ai servizi online e di e-commerce.

Ed è proprio per questo che mi trovo qui, nella veste di consulente di sicurezza in una delle mete più esotiche che abbia mai visitato.

È evidente che Dakar significa affari. Dove c'è una connessione e un servizio online, presto ci saranno anche i cyber criminali. Ma riconoscendo e affrontando in anticipo le potenziali minacce, le organizzazioni senegalesi saranno preparate e pronte. E se avranno bisogno di un supporto extra, sarò ben lieto di tornare! ■

Sicurezza umana applicata

"Se conosci il nemico e te stesso, non dovrai temere il risultato di cento battaglie."

Sun Tzu, L'arte della guerra

Autori: Anastasios Arampatzis (AKMI Educational Institute) e Justin Sherman (Duke University)

Abstract

Nel mondo odierno, sempre più interconnesso, diventiamo ogni giorno più vulnerabili. Cyber criminiali, spie, Stati canaglia sono solo alcuni degli agenti di minaccia che popolano il campo di cyber battaglia. Ciononostante, chi si occupa di sicurezza continua a rimanere focalizzato sui tecnicismi, trascurando completamente i *bias*, sia cognitivi sia culturali, che sono alla base del comportamento umano.

In questo saggio, suddividiamo la sicurezza umana applicata in tre sezioni, attingendo alle conoscenze derivanti da cyber security, cyber psicologia, teoria sistemica, social engineering, tassonomia di Bloom, teoria dell'apprendimento, economia comportamentale e scienze decisionali per capire come le aziende possono costruire la sicurezza intorno a – e per – l'uomo. Prima conosceremo il nemico, poi capiremo l'essere umano, e in conclusione proporremo delle azioni concrete che le aziende possono realizzare per rinforzare la propria cyber security.

BIO

Anastasios Arampatzis è un ufficiale dell'aviazione greca in pensione, con più di 20 anni di esperienza nella gestione di progetti di Information Technology e Cyber Security. Durante il servizio nelle Forze Armate, è stato assegnato a diverse posizioni chiave nei quartieri generali nazionali, della Nato e dell'Unione Europea.
È stato insignito di numerose alte onorificenze per la sua esperienza e professionalità ed è stato nominato valutatore certificato NATO per la sicurezza informatica. È anche insegnante certificato di informatica per il *lifelong training*.
Gli interessi di Anastasios comprendono il lato umano della cybersecurity, la psicologia della sicurezza, dell'educazione pubblica, dei programmi di formazione, e gli effetti dei *bias* (culturali, euristici e cognitivi) nell'applicazione delle politiche di sicurezza e nell'integrazione della tecnologia nell'educazione. Lo intrigano le nuove sfide, è di mente aperta e flessibile. Al momento, lavora come insegnante di informativo all'AKMI Educational Insititute.

Parte I: Il Nemico

Introduzione

I notiziari sono invasi da storie di incidenti di sicurezza e data breach che hanno divulgato i dati personali, sensibili, riservati e segreti di milioni di persone. Numerosi professionisti del settore hanno dichiarato il 2017 come il peggiore anno in materia di incidenti di sicurezza, ma le previsioni per il 2018 sono anche peggiori. In aggiunta a uno scenario di minacce che cambia rapidamente e costantemente, le tecnologie emergenti quali l'Intelligenza Artificiale, l'apprendimento automatico e il calcolo quantistico stanno cambiando radicalmente la maniera in cui l'era moderna affronta la cyber security e rendono sempre più difficile rimanere "un passo avanti".

In concreto, possiamo guardare al panorama cyber come a un campo di battaglia in cui una delle armi chiave sono le informazioni. In una società completamente permeata dall'informazione, il potere viene dal possesso e dallo sfruttamento tempestivi e puntuali di questi dati.

L'epicentro della battaglia siamo noi, gli esseri umani. Diverse analisi identificano noi umani come l'anello debole dello scenario cyber, vulnerabili a un numero infinito di tecniche di inganno e sfruttamento. Veniamo condizionati dalla situazione digitale intorno a noi, ma le nostre risposte nel contesto cyber non sono istintive e "logiche", ma sono radicalmente plasmate dalle nostre convinzioni personali, dai nostri bias, e da quello che sappiamo.

Ecco perché questo breve saggio, centrato sull'elemento umano della cyber security. Partendo dalla citazione del famoso testo di Sun Tzu *L'arte della guerra* in prima battuta parleremo dell'ambiente esterno, "il nemico", che costituisce il panorama in cui si muove la minaccia umana; nella seconda sezione, analizzeremo i bias euristici su cui si basa la risposta umana a queste

minacce; e infine, nella terza sezione, cercheremo di definire come si possa costruire intorno e per questi bias, di modo da rinforzare concretamente la cyber security umana.

Il nemico: Minacce dall'ambiente esterno

Se consideriamo l'essere umano come un "sistema" nel contesto della teoria sistemica, l'ambiente esterno è un elemento di invio input verso il processo decisionale di ogni persona. Questi input possono essere "buoni", ma possono essere anche "malevoli" e falsare il modo in cui prendiamo decisioni. Questo è il "nemico" che dobbiamo combattere per poter fare scelte migliori e rendere più sicura la sfera cyber.

La sfera virtuale

Mentre la tecnologia si evolve e modifica il nostro operato quotidiano, lo stesso avviene al comportamento umano. Psicologi come la Dottoressa Mary Aiken ritengono che le persone si comportino diversamente quando interagiscono nella sfera astratta del cyber spazio e quando invece agiscono nel mondo reale, faccia a faccia. Il termine "cyber" qui si riferisce a qualsiasi elemento digitale, dalla tecnologia Bluetooth alle auto senza conducente ai cellulari agli apparati di rete all'intelligenza artificiale e all'apprendimento automatico. Quindi: in che modo il cyber sta condizionando il nostro processo decisionale?

Minaccia numero uno: **cyber safety è un termine astratto.** Le persone comprendono più facilmente ed efficacemente i rischi connessi al guidare ubriachi che quelli legati all'avere connesso ad Internet un computer non patchato. Di conseguenza, le persone spesso non riconoscono un rischio o l'elemento lanciato per attrarle, e credono di essere meno vulnerabili degli altri. Come dice Ryan West, molta gente crede di essere meglio del guidatore medio e di poter vivere una vita più lunga della media. Sono anche convinte di essere meno esposte ai pericoli dei prodotti di consumo rispetto alla media. Quindi è ragionevole pensare che chi usa un computer abbia lo stesso set preconfigurato di convinzioni e creda perciò di essere meno esposto alle vulnerabilità informatiche. Inoltre la scelta di sicurezza (per esempio, la cifratura delle mail) spesso non dà risultati visibili, così come tipicamente non sono "visibili" le minacce (per esempio, qualcuno che vuole intercettare la posta aziendale). La ricompensa per il comportamento più sicuro, quindi, è nel fatto che non accade nulla di male: ma questo, per sua stessa natura, non mette le persone nella condizione di considerare la sicurezza come un valore quando devono comparare costi, benefici e rischi. Se infatti paragoniamo l'astratta ricompensa (protezione) di essere più sicuri rispetto alla ricompensa concreta di vedere, ad esempio, un attachment, il risultato è sfavorevole per la sicurezza. Questo è specialmente vero quando un utente non sa quanto sia alto il proprio livello di rischio, o crede di essere meno esposto della media.

Il cyber crea dipendenza. Uno studio ha dimostrato che l'utente medio controlla il proprio smartphone più di 1500 volte a settimana. Ed è la natura stessa della rete ad intensificare questo fenomeno. Internet è sempre lì,

BIO

Justin Sherman è al secondo anno alla Duke University dove si sta specializzando in Informatica e Science Politiche, dopo aver conseguito una certificazione in Mercati e Management. Si concentra su tutto ciò che è cyber, compresa la sicurezza, la guerra virtuale, l'etica, il terrorismo, la censura e la governance.
Svolge ricerche in materia di sicurezza tecnica presso la facoltà di Informatica, spaziando dal network neurale fino alla privacy mobile, il tunneling cifrato e la sicurezza dell'Internet of Things. Svolge ricerche in materia di policy tecnologica con la Sanford School of Public Policy, occupandosi di tecnologia e povertà, disinformazione e regolamentazione internazionale in materia di tecnologie. È anche cyber ricercatore in un dipartimento della North Carolina State University, appoggiato dal Ministero della Difesa, dedicato alla sicurezza informatica e nazionale.
Justin è certificato in policy di sicurezza, gestione della sicurezza informatica aziendale, protezione delle infrastrutture, social engineering, privacy, information security, pianificazione della continuità, e pianificazione della sicurezza nazionale da organizzazioni quali FEMA, l'Istituto Nazionale della Salute, il Dipartimento della Sicurezza Interna e il Dipartimento della Difesa degli Stati Uniti D'America. È stato pubblicato numerose volte, miscelando informatica, policy analysis, scienze decisionali, comportamento politico, sociologia dei mercati, filosofia, teoria bellica, politica estera e diritti umani per comprendere la tecnologia in maniera utile ed efficace. Ha anche esperienze come insegnante di informatica, sviluppatore dei piani di studio STEM e technical trainer. Potete saperne di più su di luì o contattarlo attraverso la sua pagina Linkedin linkedin.com/in/justinwsherman.

aperto, 24/7, pieno di promesse, contenuti e dati. È anche colmo di **ricompense a intermittenza**, che sono molto più efficaci della **ricompensa continuativa** nel creare dipendenza. Ricordate il film *C'è posta per te* con Tom Hanks e Meg Ryan? A un certo punto, Tom Hanks dice che non c'è nulla di più potente delle semplici parole "Hai una mail". Questa è la vera essenza della dipendenza digitale – controlliamo i nostri device perché qualche volta siamo abbastanza fortunati da essere ricompensati con una notifica.

Quando qualcosa dà dipendenza, tendiamo a fare scelte irrazionali ogni qualvolta dobbiamo prendere decisioni che lo coinvolgono in qualche modo. Cerco quindi sono; ottengo like quindi esisto. Controlliamo la nostra mail, ora, e di nuovo, e di nuovo.

Questo ci porta dritti a un'altra minaccia, **il tempo che passiamo online.** Quando controlliamo il cellulare, o anche mentre stiamo scrivendo questo documento, ci

troviamo effettivamente in un ambiente diverso; siamo andati da un'altra parte rispetto al tempo e allo spazio del mondo fisico. Perché il cyberspace è uno spazio distinto, molto diverso dallo spazio concreto in cui si trovano le nostre famiglie, le nostre case, il nostro lavoro. Molti di noi hanno provato la sensazione di "aver perso il senso del tempo" mentre navigavano online, perché non abbiamo ancora imparato a tenere traccia del tempo nella sfera virtuale. E questo ha conseguenze profonde su come ci comportiamo e le decisioni che prendiamo nel virtuale. (E per quanto riguarda la sicurezza, più tempo significa più rischi.)

In ultima battuta, dobbiamo tenere in considerazione la **natura libertaria di Internet**. Internet è progettata per essere libera. Ma dove finisce la libertà e inizia il totalitarismo? Quali e dove sono i confini fra libertà e corruzione? La "libertà di parola" è fake news? E chi decide che certe opinioni sono fake news, ammesso che qualcuno debba e possa deciderlo? Allo stesso modo, l'interesse personale come può surclassare quello della più ampia community virtuale? L'idea della libertà online è piuttosto controversa, e solleva diverse questioni etiche, ma al momento esiste davvero poca regolamentazione.

Dovrebbe essere chiaro che il nostro ambiente ha un impatto sui nostri processi decisionali. I nostri istinti si sono evoluti attraverso la storia per gestire le interazioni faccia a faccia con altri esseri umani, ma una volta che ci addentriamo nella sfera virtuale, questi istinti non bastano più.

La tecnologia in continua evoluzione

Man mano che i gadget e i device cambiano, cambia anche la sfera virtuale, e di nuovo questo comporta delle conseguenze su di noi. Più cambiamenti portano a più situazioni nuove, creando più confusioni.

Fino a diversi decenni fa, il passo di qualsiasi rivoluzione tecnologica era tale da consentire agli uomini di assorbire il cambiamento e integrarlo nella loro quotidianità. Nel corso degli ultimi venti anni, invece, l'evoluzione della tecnologia digitale è diventata così frenetica che le persone non riescono a starle dietro. Non dobbiamo certo elencare tutte le parole d'ordine e i tormentoni che nascono ogni singolo giorno come riprova di questo argomento.

Persino i "nativi digitali", per usare la discussa terminologia di Marc Prensky, a volte si sentono spaesati di fronte alla tecnologia sempre mutevole. Non abbiamo ancora trovato un modo per utilizzare a nostro favore questa tecnologia; non sappiamo con certezza come usarla efficacemente e sicuramente; e non sappiamo quali saranno le conseguenze a lungo (e breve, anche) termine di tutte queste neonate tecnologie.

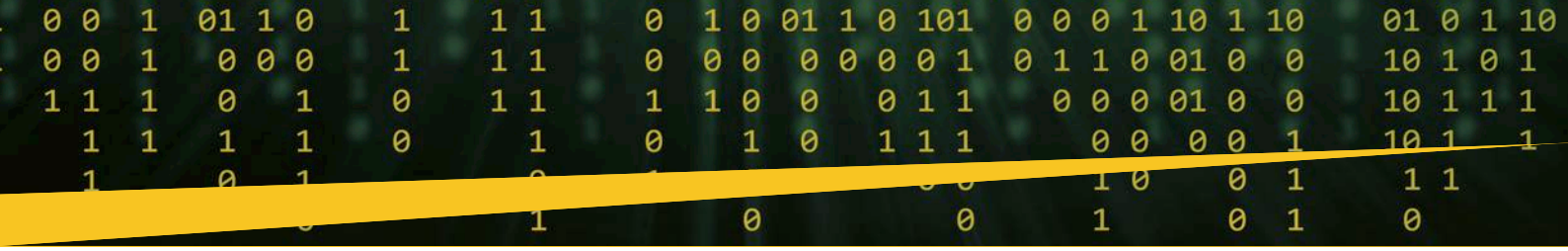
Certamente vi sono buone pratiche per integrare queste tecnologie nelle nostre vite, ma vi sono anche cattive pratiche che molti di noi seguono allo stesso modo. Oltretutto, la tecnologia ha creato anche una rivoluzione senza precedenti in materia di creazione di contenuti digitali. Questo solleva molti interrogativi: quali sono le implicazioni dell'esporre così tanti dati sensibili online? Chi ne trae beneficio? Possiamo proteggere i nostri asset più preziosi, o stiamo aprendo le nostre case ai peggiori criminali che potrebbero cancellare le nostre vite con un solo click? (Ricordate il film *The Net* con Sandra Bullock?)

La tecnologia non è buona o cattiva di per sé, è neutrale; semplicemente si interpone, amplifica e cambia il comportamento umano. Può essere usata bene o male dal genere umano; per molti versi, non è diverso da come decidiamo di guidare l'auto o usare l'elettricità o l'energia nucleare. Ogni tecnologia può essere usata male. Di qui, la domanda centrale: qual è l'etica universalmente accettabile per l'utilizzo della tecnologia cyber?

L'educazione

L'educazione è ovviamente uno dei fattori che plasmano il comportamento umano. Abbiamo letto un numero infinito di articoli sulla necessità di investire nella formazione. A livello macroscopico, la diffusa mancanza di educazione può trasformarsi in ignoranza, autoritarismo, o persino anarchia. L'attuale mancanza di una formazione esaustiva riguardo la sfera virtuale può creare problemi al modo in cui le persone percepiscono la dimensione cyber, i suoi rischi e le sue minacce.

Un altro tema è l'efficacia dell'educazione digitale già esistente. L'educazione dovrebbe avere come obiettivo la risposta ai "perché" e non solo ai "come" della sicurezza. Dovrebbe puntare a una comprensione profonda, a far rimanere le cose che vengono insegnate, e naturalmente dovrebbe



essere continuativa. Sfortunatamente, non è questo il caso. L'approccio pedagogico tipico si basa sul rinforzo positivo quando facciamo qualcosa di "giusto". In altre parole, quando facciamo bene qualcosa veniamo premiati. Nel caso della sicurezza, però, quando l'utente fa qualcosa di "giusto", l'unica ricompensa è che diminuiscono le probabilità che accada qualcosa di male. È un risultato piuttosto astratto, che non fornisce né gratificazioni né ricompense immediate, che sono entrambi due rinforzi importanti nella conformazione di un comportamento.

Dovremmo esaminare anche il caso opposto, come viene plasmato il nostro comportamento dal rinforzo negativo quando facciamo qualcosa di "sbagliato". Normalmente, quando facciamo qualcosa di male in un contesto educativo, ne subiamo le conseguenze. Nel caso della sicurezza, invece, il rinforzo negativo per un cattivo comportamento non è immediatamente evidente. Può essere posticipato di giorni, settimane, mesi, ammesso che arrivi mai. (Pensate a una violazione della sicurezza o a un furto d'identità, per esempio.) Il rapporto causa-effetto si impara meglio quando l'effetto è immediato, mentre la scelta anti-sicurezza spesso non ha conseguenze immediate. Questo rende difficile promuovere la comprensione delle conseguenze, tranne nel caso di disastri spettacolari.

Inoltre, bisogna tenere conto del fatto che fattori quali forza di volontà, motivazione, percezione del rischio, costi e opportunità sono spesso più importanti della mancanza di conoscenza in sé.

Social Engineering

Gli attacchi via *social engineering*, orchestrati per lo più attraverso messaggi di phishing, rimangono una minaccia persistente che consente agli hacker di aggirare i controlli di sicurezza. Sfruttando le loro abitudini, motivazioni e bias cognitivi, è possibile manipolare le persone perché rivelino informazioni confidenziali. Le ricerche sul phishing si concentrano in particolare sulla capacità dell'utente di rilevare anomalie strutturali e fisiche nelle mail, come ad esempio errori di ortografia o le differenze fra l'URL mostrato e quello incorporato nel codice HTML. Ma le persone spesso "processano" una mail usando modelli mentali o euristici, e quindi trascurando gli indizi che mostrano l'inganno. Inoltre, le abitudini, le necessità e i desideri della gente la rende vulnerabile agli attacchi di phishing che promettono ricompense.

La sensibilità rispetto ai messaggi di phishing è cresciuta molto fra gli utenti, ma altrettanto è cresciuta la capacità degli attaccanti di falsificarli. Oggi, gli hacker progettano i messaggi in modo da scatenare reazioni (paura, rapacità, altruismo) e spesso scelgono come obiettivi dei gruppi specifici cui fare richieste specifiche. A volte arrivano persino a personalizzare il messaggio inserendo informazioni personali del destinatario *(spear phishing)*. Ad esempio, è stato rilevato un nuovo tipo di phishing sulle app per appuntamenti: un bot che si spaccia per un utente avvia una conversazione con un altro utente (la vittima) e, dopo qualche scambio, gli invia un link malevolo, spesso con una foto, nel tentativo di convincerlo a cliccarlo. Le ricerche mostrano che questo tipo di attacchi *spear* sono più efficaci del phishing generico, che punta a una popolazione più ampia.

Gli attori malevoli

In questi giorni, il cybercrime è più organizzato che mai. I cyber criminali sono forniti di strumenti e fondi adeguati, oltre ad avere le conoscenze necessarie per portare a termine il lavoro. Ma per capire fino in fondo i cyber criminali, dobbiamo sapere una cosa sopra tutte le altre: le loro motivazioni.

I cyber criminali sono interessati al denaro. Usano i ransomware per estorcere denaro, o sottraggono i dati che possono essere rivenduti sul dark web. Il loro modus operandi passa principalmente per le campagne di phishing, che sono solitamente a basso costo e possono dare un ritorno dell'investimento inziale davvero sbalorditivo. Tipicamente, queste campagne sono utilizzate per distribuire malware (spesso ransomware), e le mail si fondano in maniera significativa sul social engineering. Ad esempio, ai destinatari è spesso richiesto di aprire o inoltrare l'allegato, di solito falsi documenti di lavoro, che all'apertura attiva il software malevolo.

A differenza dei cyber criminali, gli hactivisti non sono motivati dal denaro, quanto piuttosto dalla vendetta. Gli hactivitsti lavorano da soli, rendendo molto difficile predire i loro attacchi o rispondere velocemente. A volte, gli hactivisti sono interni, che sanno come bypassare le misure di sicurezza dell'organizzazione, ma il rischio maggiore è sempre connesso al fatto che è difficile risalire a chi siano e a quando attaccheranno, e spesso anche a perché lo facciano. Se non altro sappiamo che il loro modus operandi preferiti è il DDoS *(distributed denial of service)*, perché mette in imbarazzo le vittime.

Negli ultimi anni, abbiamo ricevuto notizie in merito ad attacchi e cyber spionaggio finanziati dai governi. In maniera ben poco sorprendente, gli attaccanti stipendiati dai governi non sono interessati ai nostri soldi: vogliono i nostri dati, e per farlo devono riuscire a garantirsi un accesso costante ("persistente") alle nostre infrastrutture IT. Se un'azienda opera in un campo particolarmente sensibile, in cui i dati sono meticolosamente salvaguardati (ad esempio, infrastrutture critiche o voti elettorali), allora rischia seriamente di essere oggetto di attenzione da parte di hacker "governativi". In estrema sintesi, visto che c'è così tanto online, i gruppi "governativi" lavoreranno simultaneamente su molteplici vettori d'attacco. In questo modo, possono raccogliere dati sensibili lungo un ampio arco temporale, invece che puntare a semplici "raid".

Conclusioni

Quello virtuale è il campo di battaglia in cui possono collidere interessi diversi. Nella foschia e fra la polvere sollevata da questa collisione c'è l'essere umano, che è il collettore di molti input, buoni e cattivi, in grado di modificare il modo in cui si comporta e reagisce,

Ma anche senza tenere in considerazione questi input esterni, tutti i bias cognitivi ed euristici di ogni persona giocano un ruolo primario, di cui parleremo nella seconda sezione.

Parte II: L'essere umano

Introduzione

Nella prima parte di questo saggio, abbiamo parlato del "nemico", l'ambiente esterno che crea le minacce cui gli esseri umani devono rispondere.

In questa seconda sezione ci concentreremo sulle convinzioni e i bias che plasmano le nostre azioni nel panorama cyber. Facendo riferimento a quanto sappiamo in materia di economia comportamentale, cyberpsicologia, social engineering e scienze decisionali, risponderemo a una delle domande fondamentali della cyber security: perché l'uomo è l'anello debole?

L'essere umano

I fattori che tengono in piedi la sicurezza informatica di un'azienda sono innumerevoli: dai firewall e gli standard di crittografia ai protocolli di reportistica degli incidenti e a tutta la cultura di sicurezza. Molte organizzazioni cercando sempre di rimanere in pari, quando si parla di tecnologia informatica solida, ma i dipendenti rimangono per lo più vulnerabili.

Gli esseri umani sono fallibili sia nel ricordare le informazioni (ad esempio, di un corso d'aggiornamento) sia nell'usarle (ad esempio, prendere decisioni quando usano la tecnologia), il che mette tutte le grandi organizzazioni a rischio. I numeri lo mostrano con chiarezza: le statistiche dell'anno scorso indicano che più di due terzi di tutti gli incidenti di sicurezza sono stati causati da errore, utilizzo o manipolazione umana, come nel caso di attacchi di *phishing* e *spear phishing*. Gli hacker sono consapevoli della vulnerabilità rappresentata dal fattore umano, e sono ben felici di poterla sfruttare, come abbiamo spiegato nella Sezione I.

Euristica delle decisioni e cyberpsicologia

Il nostro cervello è evoluzionisticamente programmato per diminuire il tempo che dedichiamo alle decisioni attraverso l'uso dell'euristica delle decisioni: in pratica, un sistema semplice ed efficace di regole che guidano il nostro giudizio. Ma mentre queste scorciatoie cognitive sono di grande beneficio per diverse ragioni, dall'altra parte ci lasciano esposti ai bias euristici, che possono farci incorrere in errori di giudizio e supposizioni sbagliate quando valutiamo un set di decisioni. Sono fondamentali per capire come si muove l'essere umano nella sfera virtuale.

Diversa ma legata al discorso è la cyberpsicologia, un campo di studi emergente dedicato alla comprensione di come gli essere umani interagiscono con, e sono modificati da, la tecnologia. Mentre le scienze decisionali studiano i processi decisionali e le loro applicazioni a tutto tondo, la cyberpsicologia è specificatamente dedicata alla tecnologia, e si interroga su quali comportamenti cambino quando entriamo nella sfera virtuale e quali no. Non è probabilmente una grande sorpresa scoprire che è più frequente il caso in cui il comportamento cambia significativamente (addirittura, a volte, radicalmente) appena ci sediamo di fronte allo schermo. L'esperta del settore D.ssa Mary Aiken chiama questo mutamento repentino **l'effetto cyber**, e vi riconduce tutto, dall'**amplificazione comportamentale** alla **disinibizione online**.

Ma ci torniamo fra poco.

Password e login

Gli esperti di sicurezza e i professionisti dell'IT raccomandano continuamente le best practices per l'uso delle password, eppure la maggior parte delle persone non le seguono. E questo perché creare e conservare una password rappresenta una sfida significativa per molte persone.

Prima di tutto, la maggior parte di noi tende a scegliere password **memorizzabili**, siano i nomi dei nostri familiari, le date importanti, o il

titolo del nostro film preferito. Le scegliamo memorizzabili perché ne usiamo un grande numero; è praticamente impossibile per chiunque memorizzare tutte le password di tutti i nostri account, email, social media, servizi di streaming, siti di e-commerce, database lavorativi e home banking.

Questa tendenza a creare password memorizzabili c'era quando le vecchie linee guida del NIST suggerivano di usare insiemi casuali di lettere, numeri e simboli, e c'è anche ora che il NIST suggerisce l'uso di passphrase lunghe e complesse. Semplicemente, è più facile ricordare **informazioni rilevanti per sé** che un insieme random di lettere e numeri. Quindi sceglieremo più probabilmente password come *125elmST* (un vecchio indirizzo) o *johnlucyjacksarah* (i nomi dei figli) che non *e7@4j8!9*.

Indubbiamente bisogna fare dei compromessi fra robustezza della password, mutevolezza e facilità di memorizzazione: avere molto password memorizzabili è un compromesso rispetto a una sola password molto complessa (e non memorizzabile). Il problema però è che le password

memorizzabili sono facili da "craccare" per qualcuno che pratichi social engineering. Pochi minuti con Kali Linux o qualsiasi altro strumento di penetration test mostreranno rapidamente la pletora di software disponibili per questo scopo, da dizionari pre-assemblati di password popolari a script che inseriscono le informazioni di un target (nome, coniuge, domicilio) all'interno di dizionari di password customizzati. I nostri prevedibili comportamenti lasciano noi, e per estensione i nostri amici, familiari, impiegati e colleghi, vulnerabili alla possibilità di essere hackerati.

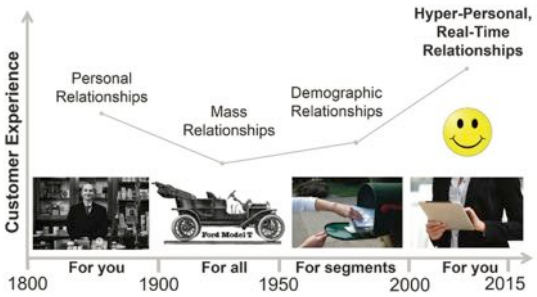
Quando veniamo costretti a cambiare le nostre password, che ce lo chieda un sistema operativo o la politica aziendale, tendiamo a sovrapporre le nuove sulle vecchie. Se la mia password attuale è *strongP@ssw0rd!123*, è probabile che quella nuova sarà qualcosa come *strongP@ssw0rd!456* o anche *strongerP@ssw0rd!123*, così da non dover memorizzare una nuova frase. Abitudini e schemi ricorrenti, in particolare nel cyberspazio, sono importanti, da cui deriva la definizione di **bias dello status quo**, o preferenze di default (in altre parole, lasciare le cose come stanno anziché cercare di gestire il cambiamento). Di nuovo, però, questo comportamento prevedibile rende gli essere umani vulnerabili. Se un hacker sta usando nell'ombra le credenziali di un impiegato, e all'improvviso si accorge (poiché non riesce più ad accedere) che la password è stata cambiata, probabilmente farà leva sulla conoscenza di questo bias e farà qualche tentativo con password simili alla precedente, cambiando numeri o lettere, come negli esempi che abbiamo appena fatto. In questo modo, la lunghezza della password diventata immediatamente ininfluente.

Riconoscere le minacce: Phishing, social engineering, e altro

I bias euristici ci rendono incredibilmente vulnerabili – e inefficaci – quando si parla di individuare le minacce informatiche, e sono peggiorate dal fatto che non possiamo contare sui nostri "istinti" consueti né sul **linguaggio** noto quando entriamo nella sfera virtuale. È a questo che mirano gli attaccanti, come abbiamo detto prima.

Gli esseri umani vogliono avere fiducia, e questo è mostrato con chiarezza dall'efficacia degli attacchi phishing. Possiamo essere istruiti a riconoscere come è fatta una mail di phishing; possono dirci di non fidarci mai di una mail inviata da un mittente sconosciuto; possono persino insegnarci a non fidarci di email sospette inviate da mittenti noti. Ma in pratica, questo modello non funziona. Nella nostra casella di posta ogni anno passano molte mail di phishing (confermato anche dai dati sulle violazioni di sicurezza nelle aziende), ma la maggior parte della posta elettronica che riceviamo non lo è. Ogni volta che apriamo una mail apparentemente sospetta che si rivela sicura, che ci piaccia o meno stiamo cadendo in un **bias di conferma**. L'idea preconcetta che non dobbiamo controllare ogni mail si rinforza ogni volta che ne apriamo una sospetta senza conseguenze negative. In questo modo, l'attenzione prestata a ogni mail sospetta diminuisce col tempo, aumentando le possibilità che un attacco di phishing avvenga con successo.

Anche la rappresentatività ricopre un ruolo, qui. Quando svolgiamo ripetitivamente un compito, il nostro cervello categorizza insieme la piccole possibili variazioni, di modo da ridurre il tempo decisionale. Per esempio, se un manager invia ogni venerdì una mail di "Recap settimanale", gli impiegati non noteranno un "recap settimanale", mandato di venerdì, che non proviene però dall'indirizzo email del capo. La nostra tendenza a raggruppare erroneamente le nuove situazioni all'interno di confini già noti può essere letale; è per questo



che gli esperti di social engineering sono sempre alla ricerca di modi in cui inserire URL, documenti e altre feature malevole all'interno di pattern comportamentali noti.

Aggiungere il concetto di **disinibizione online** al quadro mostra quando siamo vulnerabili agli attacchi di social engineering: i primi risultati delle ricerche di cyberpsicologia mostrano che siamo molto più avventati online che non nelle nostre interazioni vis-a-vis; la D.ssa Aiken arriva a paragonare alcuni nostri comportamenti virtuali a uno stato di ubriachezza, visto che ci fidiamo più facilmente del prossimo e riveliamo più velocemente informazioni personali. Questo, unito alla **iper-interazione virtuale** (diminuzione delle barriere sociali all'intimità e allo scambio di informazioni) e alla **sindrome dello straniero sul treno** (la tendenza a rivelare informazioni sensibili con coloro che pensiamo di non vedere mai più), mostra quanto siamo già inclini a condividere troppe informazioni online, e il tutto è aggravato dagli attori malevoli capaci di sfruttare i nostri bias euristici. Il modo in cui ci comportiamo online, e il modo in cui decidiamo su cosa cliccare e cosa condividere, sono tutte ragioni che concorrono a rendere l'uomo l'anello debole della catena virtuale.

Legato a queste idee c'è un altro elemento con cui tutti facciamo i conti: il **bias ottimista**, la convinzione di navigare il mondo meglio di tutti gli altri. Nel mondo fisico, questo succede in continuazione. Tendiamo a esentarci da regole, politiche e standard il cui rispetto pretendiamo dagli altri perché riteniamo di esserne al di sopra; per esempio, molti tendono a scrivere messaggi al cellulare mentre guidano, nonostante i numeri che mostrano con forza come questo sia pericolosissimo per sé e per gli altri, perché reputano che *loro*, a differenza degli altri, siano multitasking. (E diversi studi, ovviamente, mostrano come il "multitasking" nella sua accezione più piena sia impossibile.) E questo si trasferisce pari pari nella dimensione virtuale, dove tutti classifichiamo le nostre performance sopra la "media" e quindi cadiamo al di sotto degli standard minimi di sicurezza informatica. Se un impiegato provoca un incidente di sicurezza a causa di una password debole, con ogni probabilità lo criticheremo; tuttavia, con la stessa probabilità, ci concediamo di salvare le password nel browser o di aggirare l'autenticazione multifattore *senza* criticarci. Allo stesso modo, un impiegato può essere ben consapevole dei pericoli rappresentati dal

social engineering ma non prestare attenzione a evitare gli attacchi di phishing, semplicemente perché ritiene di non averne bisogno, e anche se lo critichiamo, molti di noi probabilmente fanno la stessa cosa.

Gli esseri umani sono anche esposti all'effetto **recency**, che ci rende più sensibili alle informazioni fornite di recente. Se ad esempio un impiegato segue un corso di tre ore sui pericoli del malware, sarà più attento a ciò che scarica da Internet che non alle email di phishing. Questo sembra ovvio, ma il bias euristico che vi sottintende è critico per la vulnerabilità umana: la minaccia "recente" sarà la minaccia prioritaria. Di conseguenza diventa importante l'ordine in cui si fa formazione.

Il **bias di frequenza**, o il favorire le informazioni ribadite, ha conseguenze simili su ciò che ci portiamo via dalla formazione e sensibilizzazione. È sensato che più un argomento è discusso più ne è percepita l'importanza, ma in materia di sicurezza semplicemente ci sono troppo argomenti per poterli coprire tutti in maniera adeguata, e questo è un problema. Se un'azienda organizza 5 ore di formazione sul tema della cifratura delle mail o la creazione delle password, ma ne dedica solo 3 agli attacchi di phishing e social engineering, con ogni probabilità i dipendenti riterranno prioritario difendersi dai primi, mentre il social engineering rappresenta un rischio più grave. Bilanciare il tempo dedicato a una minaccia informatica con la percentuale di sua concretizzazione è una questione complessa (di cui parleremo nella prossima sezione), ma dobbiamo tenere in considerazione questo bias.

Conclusioni

Il comportamento umano nella sfera virtuale è incredibilmente fallace, dalle vulnerabilità delle decisioni euristiche ai bizzarri comportamenti che adottiamo solo perché abbiamo poca familiarità con la tecnologia. Comprendendo meglio le scienze decisionali, l'economia comportamentale e la cyberpsicologia, possiamo migliorare la sicurezza umana applicata. Quindi, avendo analizzato sia il "nemico" sia "l'umano", la terza e ultima sezione si concentrerà sul "vincere la battaglia", ovvero definire la sicurezza informatica tenendo a mente la componente umana.

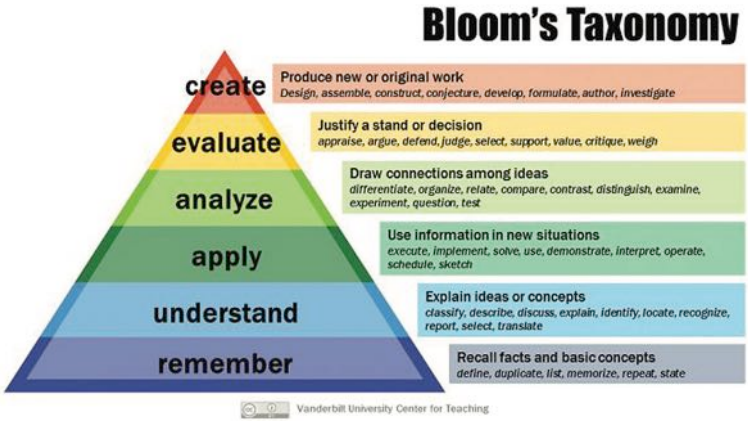
Parte III: Vincere la battaglia

Introduzione

La prima parte di questo saggio, "Il Nemico" era incentrata sull'ambiente esterno e le minacce che introduce nel panorama virtuale, mentre la seconda parte "L'essere umano" ha discusso i bias euristici e i preconcetti che definiscono la risposta umana a queste minacce. Nella parte conclusiva, vogliamo affrontare come "non temere il risultato di cento battaglie" o, in altre parole, come definire le politiche di sicurezza intorno e per l'essere umano.

Background teoretico

Diversi decenni fa, lo psicologo dell'età evolutiva Jean Piaget dichiarò che "il principale scopo dell'educazione è formare uomini che siano capaci di fare cose nuove, non ripetere semplicemente ciò che hanno fatto le altre generazioni – uomini che siano creativi, inventivi e portati alla scoperta".



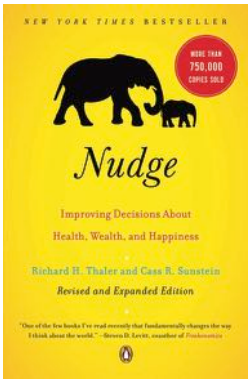
Partendo da qui, possiamo guardare all'apprendimento come a un processo di acquisizione e costruzione di conoscenze con forti componenti sociali ed esperienziali.

La ricerca in materia di formazione ha mostrato che le persone possono imparare più efficacemente e approfonditamente attraverso l'impegno, la motivazione, la cooperazione, la collaborazione la partecipazione in esperienze reali. Quindi, i metodi convenzionali di insegnamento non possono soddisfare i requisiti di apprendimento odierni. Costruire e condividere conoscenza arricchisce l'efficacia dell'insegnamento e il curriculum, con una significativa distanza dall'educazione burocratica che preferisce la quantità alla qualità, e guarda alla motivazione innata. Attraverso tecniche e metodologie quali forum di discussione ed esercizi concreti, piccoli gruppi di persone possono sviluppare il pensiero critico, imparare a mobilitarsi verso un obiettivo comune, e fare affidamento su un'intelligenza collettiva che è superiore alla somma di quella dei singoli individui.

Secondo la tassonomia di Bloom, tuttavia, l'insegnamento non dovrebbe concentrarsi solo sul trasmettere informazioni, ma anche sulla loro applicazione. Usare vecchie informazioni per risolvere nuovi problemi è essenziale per memorizzare ciò che si apprende e sviluppare nuova conoscenza. Prevedibilmente, si attiva molto velocemente un ciclo ripetitivo, in questo: le vecchie conoscenze vengono rinforzate dall'applicazione, e l'applicazione richiede nuove conoscenze da applicare e via così. Il prodotto di questo processo è spesso chiamato **deep learning**. La ludicizzazione e la simulazione sono due esempi di applicazione del processo di deep learning.

Default e "spinte gentili"

Nel loro testo del 2009 *Nudge. La spinta gentile*, gli economisti Richard Thaler e Cass Sunstein, hanno definito l'idea del **paternalismo libertario**;



un modello decisionale dove nessuno vede le proprie scelte limitate o falsate (l'elemento libertario), ma in cui, inquadrando le scelte in un certo modo, i creatori possono aiutare le persone a selezionare l'opzione migliore (l'elemento paternalista). In sostanza, l'idea è di **spingere gentilmente** gli individui nella giusta direzione senza limitarne la libertà. Ci sono molti modi di ottenere questa "spinta gentile", per esempio ordinare in maniera diversa le opzioni e aumentare la quantità di informazioni di base disponibili, ma noi vogliamo focalizzarci su un metodo in particolare: cambiare le impostazioni predefinite.

Le **impostazioni predefinite** sono incredibilmente potenti quando entrano nel processo decisionale, come mostrano i tanti studi di scienze decisionali ed economia comportamentale. A causa del **bias dello status quo** – vale a dire, la nostra avversione a mettere impegno nel cambiamento – molti di noi probabilmente sceglieranno di adeguarsi alle impostazioni predefinite in ogni scenario decisionale. *Nudge. La spinta gentile* evidenzia quanto questo sia vero in ogni campo, dai buffet delle sale refettorio dei college ai piani pensionistici delle aziende. Per tutte queste ragioni, la **sicurezza-di-default** è una delle maniere più efficaci di "vincere la battaglia" quando parliamo di sicurezza umana applicata. Rendere la sicurezza informatica lo status quo garantirà complessivamente un comportamento più sicuro, perché molti utenti rimarranno ancorati alle impostazioni predefinite.

L'idea del "default" ha molte implicazioni nel modo in cui le aziende progettano, svolgono e rinforzano la formazione in materia di sicurezza, ma di questo parleremo fra poco, per ora concentriamoci sul modo in cui le organizzazioni possono inserire la sicurezza di default nella loro catena tecnologica.

Attivare la cifratura più robusta possibile su tutti i device acquistati per la vostra organizzazione, smartphone, laptot, sensori IoT. Installare software di crittografia, e impostarli come predefiniti sui sistemi di comunicazione, da Signal a PGP. Limitare l'accesso a Internet (ad esempio, ai soli siti relativi alle mansioni lavorativi) e fare in modo che tutti gli account abbiano il set minimo di privilegi necessari allo svolgimento di attività base (ad esempio, impedire l'installazione di software). Attivare i filtri sulle email, impostare l'autenticazione multifattoriale, e definire i requisiti minimi delle password. Configurare i software di rimozione malware, firewall interni ed esterni, e la sospensione automatica delle sessioni dopo un periodo di inattività. Tenere costantemente sotto controllo le nuove linee guida di settore e le ricerche più recenti per mantenere sempre aggiornata la sicurezza di default – per esempio, come si configura una password robusta. Ma soprattutto, evitate che i dipendenti debbano gestire complicate e fastidiose attività di controllo, quando possibile: se devono accumulare malumore perché chiedete loro di verificare due volte che le loro USB personali non siano state hackerate, semplicemente vietatene l'uso. In uno scenario di sicurezza di default, anche i dipendenti e gli utenti sono più protetti.

È importante tenere presente che questi meccanismi di sicurezza di default non dovrebbero essere proposti come scelta libera. La cifratura e l'autenticazione multifattoriale sono due classici esempi per i quali non dovrebbe sussistere l'opzione out: i dipendenti non dovrebbero poter disattivare la cifratura o diminuirne il livello di robustezza, così come non dovrebbero poter utilizzare l'autenticazione a fattore singolo (username e password). Quando si parla di sicurezza, l'assenza dell'elemento libertario funziona meglio.

Euristica delle decisioni, sistema di feedback e formazione sulla sicurezza

Come detto in precedenza, i corsi di formazione e aggiornamento sulla sicurezza al momento non sono adeguati ad affrontare le minacce provenienti dal cyberspazio, così come i bias cognitivi ed euristici che guidano il nostro comportamento online. Anche all'interno di sistemi progettati in un'ottica di sicurezza di default, non siamo in grado di proteggerci da situazioni in cui a) le aziende *non possono* configurare la sicurezza come impostazione predefinita, perché il controllo finale spetta al fattore umano e b) il fattore umano *modifica* quell'impostazione, rendendo il processo meno sicuro.

La soluzione classica (e più diffusa al momento) a questo problema è quella **di imporre una chiara politica di sicurezza aziendale**, per esempio gli utenti non possono utilizzare supporti USB esterni. Questo sembrerebbe efficace, perché la struttura aziendale incentiva intrinsecamente la compliance a queste politiche… giusto? Sbagliato. In un'ottica umana, questo approccio è con **ogni probabilità destinato a fallire** per diverse ragioni.

- Gli utenti non rispetteranno la policy perché non comprendono la gravità del rischio.
- Potrebbero non conoscere la policy o averla dimenticata.
- Potrebbero insorgere situazioni contingenti in cui gli utenti hanno necessità di ricorrere un device USB, e quindi opteranno per un'eccezione funzionale (convenienza prima che sicurezza).
- Gli esseri umani sono vittime del **bias ottimista** – pensano di essere migliori di altri in certe cose – e quindi si auto-esenteranno dal comportamento sicuro anche quando funzionalità e convenienza non sono parte dell'equazione.
- Se i dipendenti violano la policy una volta e non ci sono conseguenze negative, lo fanno di nuovo.

Tutto questo senza nemmeno prendere in considerazione le altre questioni legate agli attuali metodi di formazione, che abbiamo discusso altrove.

La maniera più sicura di prevenire il rischio, quindi, è **eliminare l'utente dall'equazione**. Ma sarebbe come amputare un braccio dolente. Non possiamo separare gli umani dalla tecnologia, o la tecnologia dagli umani, per cui, sebbene in teoria funzionerebbe, in pratica è infattibile.

Quindi la domanda rimane: cosa possiamo fare in merito alle questioni sottese della percezione del rischio e della diffusione della responsabilità (da cui possono derivare molti altri rischi)? In questi casi è necessario aumentare la consapevolezza degli utenti in merito alle tematiche di sicurezza e coinvolgerli attivamente nel processo di sicurezza, senza creare un ambiente paranoico. In breve: dobbiamo progettare formazione e politiche sulla base di come sono gli esseri umani.

Awareness e programmi di formazione sono meccanismi importanti per diffondere la cultura della sicurezza in un'organizzazione. Puntano a stimolare comportamenti sicuri, a motivare gli stakeholder a riconoscere le problematiche di sicurezza, e a educarli a rispondere adeguatamente.

Dal momento che l'awareness e la formazione non dipendono solo dai requisiti interni dell'azienda, ma anche dai vincoli esterni, devono essere allineate a tutti i requisiti di compliance. La letteratura e le linee guida attuali del NIST e dell'ENISA al momento enfatizzano l'importanza di allinearsi anche alle necessità di business, all'architettura IT e alla cultura del luogo di lavoro.

Il target dei programmi di awareness sono tipicamente i manager anziani, il personale tecnico, i dipendenti e le terze parti (consulenti, fornitori, etc). I programmi di awareness sono essenziali perché le organizzazioni devono assicurarsi che tutti coloro che gravitano loro intorno comprendano e rispettino le politiche e procedure di sicurezza, oltre a seguire le regole specifiche per i sistemi e gli applicativi cui accedono. Ma, come abbiamo spiegato, il comportamento è fortemente influenzato dalle caratteristiche e dai bias personali, il che ha delle conseguenze sul rispetto delle politiche e procedure. Di conseguenza, l'awareness dovrebbe essere progettata per contrastare le convinzioni, i comportamenti e i bias personali.

Quanti progettano i sistemi di sicurezza dovrebbero adottare un **approccio sistemico** alla formazione, ritenuto una pratica educativa efficace. Al centro di questo approccio è l'**identificazione dei bias culturali dei partecipanti**, che può facilitare la definizione del fabbisogno e fornire un criterio alternativo di raggruppamento dei partecipanti ai programmi. Poiché i bias culturali dei singoli influenzano la loro percezione e la capacità di prendere decisioni, possono influire anche sul risk assessment svolto da ciascuno di loro. Questo non viene preso in considerazione negli attuali corsi di formazione, il che rende immensamente problematico il modo in cui poi, a corso concluso, i singoli dipendenti **archiviano** quanto appreso. Se l'insegnamento non viene inquadrato in un adeguato contesto culturale (concetto che può assumere diverse sfumature), i dipendenti non capiranno *perché* la sicurezza è così importante.

Fortunatamente, inquadrare la sicurezza informatica alla luce dei bias culturali non richiede particolari risorse addizionali. Per esempio, mentre la tecnologia dà priorità alla praticità, in molti casi gli utenti potrebbero trovare più importante l'estetica. I dipendenti potrebbero quindi scegliere la sicurezza rispetto alla praticità, è sufficiente far loro capire perché dovrebbero farlo. Capire da dove provengono i partecipanti ai corsi (per esempio, per il lavoro che svolgono è più importante la praticità, la collaborazione, la velocità, etc.) consente di posizionare sotto la giusta luce la rilevanza della sicurezza. Per esempio, un team che lavora nel campo legale potrebbe comprendere meglio la sicurezza all'interno di un quadro di rischio evitato, mentre il gruppo dei contabili capirebbe meglio le sfumature legate alla confidenzialità, integrità e autenticità del dato. Ecco perché è essenziale progettare le politiche di sicurezza tenendo presenti i bias culturali. E oltre a creare e selezionare materiale di studio di questo tipo, è importante anche creare una **solida cultura della sicurezza aziendale.**

Sulla stessa falsariga, le aziende dovrebbero creare un **sistema concreto di feedback** durante e dopo i corsi di aggiornamento: un sistema di feedback debole (quello in cui in cui le scelte pro-sicurezza non ottengono alcuna ricompensa visibile, a parte il complimentoso "congratulazioni, non ti hanno hackerato!") non spinge o incentiva i dipendenti ad adottare comportamenti sicuri. Durante la formazione, lo strumento più efficace sono le "storie di successo" in cui i controlli di sicurezza hanno prevenuto un incidente, un comportamento intelligente ha bloccato un attacco di social engineering, e una chiara politica di reporting ha limitato e contenuto un'infrazione. Dopo la formazione, sottolineare in maniera casuale il buon comportamento degli impiegati aiuta a consolidare il sistema di feedback (usare **rinforzi positivi intermittenti** aiuta anche a condizionare i comportamenti).

Svolgere **simulazioni e ludicizzazioni** durante la formazione rinforzerà ulteriormente il sistema. Ogni volta che possiamo collegare un comportamento sicuro a una ricompensa più alta – anche se in un ambiente simulato – stiamo plasmando comportamenti più sicuri nell'ambiente di lavoro. Se i dipendenti sperimentano l'importanza di controllare una mail durante una simulazione (per prevenire, ad esempio, un attacco di phishing da un concorrente estero), è più probabile che saranno propensi a farlo anche nella vita reale. Perché la presa di coscienza e l'applicazione pratica, come detto, sono incredibilmente importanti per la memorizzazione dell'informazione e la ri-applicazione pratica.

Strettamente legata al sistema concreto di feedback è la **correlazione positiva**. Le ricerche sui bias cognitivi hanno dimostrato che la capacità di giudizio individuale subisce conseguenze dall'esposizione a stimoli positivi o negativi (per esempio, la vista di volti sorridenti o corrucciati), che coloro che si occupano di scienze decisionali chiamano **affect bias**, la nostra rapida reazione emozionale a qualcosa. Ne deriva che associare i messaggi sulla sicurezza a delle immagini positive (per esempio, più clienti felici significa più profitto) è

un modo efficace di assicurarsi che gli utenti si adeguino alle vostre politiche di sicurezza. Anche ricompensare le buone performance nei test di sicurezza (siano questi programmati o no) aiuta a raggiungere questo obiettivo.

Il **bias di ancoraggio**, vale a dire la nostra tendenza a fare riferimento alla prima parte di informazione fornita su un argomento, ugualmente influenza il nostro atteggiamento verso le nuove pratiche di sicurezza. Se ai dipendenti viene detto che una password robusta è composta di almeno sei caratteri, con ogni probabilità creeranno password da sei caratteri, non si allontaneranno da questa informazione iniziale. Questo comporta conseguenze a partire dal controllo delle email fino alla navigazione online. Allo stesso tempo, siamo suscettibili al **bias di frequenza**, per cui diamo priorità ai temi su cui abbiamo più informazioni, e all'effetto **recency**, per cui diamo priorità ai temi che abbiamo studiato più di recente. Se a un utente vengono impartite cinque ore di lezione sulla creazione della password ma solo tre sugli attacchi di phishing, sarà più attento al primo che non al secondo, sebbene il secondo sia una minaccia più grave e complessa.

Poiché il nostro cervello è fortemente condizionato dall'ordine e dalla frequenza con cui ci vengono presentate le informazioni, dobbiamo progettare delle politiche di sicurezza che tengano conto di queste tendenze. Progettando per il bias di ancoraggio dovremmo presentare subito le pratiche di sicurezza migliori quando affrontiamo un argomento (le password devono essere di 12 caratteri anziché di 6); per il bias di frequenza, dobbiamo assolutamente bilanciare il tempo dedicato a un tema rispetto alla sua importanza (dedicare gran parte del tempo al social engineering); per l'effetto recency, infine, dovremmo concludere i corsi di aggiornamento parlando delle cose più importanti.

Continuando con l'ordine e la cronologia delle informazioni: gli esseri umani tendono ad attribuire maggior valore ai costi e benefici a breve termine che non a quelli a lungo termine. In altre parole, gli esperti di sicurezza dovrebbero sottolineare non solo i benefici a lungo termine e di macro livello di un comportamento sicuro (per esempio, una crescita migliore dell'azienda), ma anche i **benefici immediati**. Basta guardare le notizie per vedere una pletora di esempi utili, dall'evitare colossali perdite di denaro al prevenire un incubo per l'ufficio PR e Legale. Il pensiero dei costi immediati è efficace su noi umani.

Abbiamo già parlato dei rinforzi positivi, ma è altrettanto importante (ovviamente) punire le violazioni di sicurezza. Avere una politica aziendale non controllata o applicata è l'equivalente dell'avere leggi ma non avere un corpo di polizia. Le aziende devono controllare il comportamento dei dipendenti, oltre al comportamento di *coloro che controllano* – e prendere provvedimenti quando vengono infrante le regole. Questo si ricollega al sistema concreto di feedback e all'idea che le persone prestino più attenzione all'effetto immediato delle nostre azioni: il miglior deterrente contro l'infrazione delle regole non è la severità delle conseguenze, ma il **rischio di essere scoperti**.

Un'ultima considerazione cui badare è come **ridurre il costo umano dell'implementazione della sicurezza**. Questo ricomprende molte delle idee di cui abbiamo discusso fin qui, dalla sicurezza di default alla progettazione efficace della formazione, alla contestualizzazione delle questioni di sicurezza, e al mondo in cui indirizzare correttamente il fattore umano.

La **valutazione dei programmi di formazione** è necessaria per verificare che siano efficaci. Per valutare un programma, devono essere tenute in considerazione metriche quali la memorizzazione delle informazioni apprese

e loro usabilità. Se un programma di formazione si rivela inefficace, deve essere svolto un nuovo assessment sul fabbisogno aziendale e dovrebbero essere prese in considerazione nuove tecniche educative.

Sfortunatamente, tutte le precedenti tecniche da sole non sono sufficienti a vincere la battaglia; nonostante il titolo del nostro pezzo, presumere di essere "vittoriosi" nel più pieno senso del termine sarebbe illusorio. La sicurezza deve diventare un obiettivo strategico a livello nazionale. Richiede un approccio olistico dai governi, dai politici, dagli esperti del settore fino ai cittadini, consumatori e studenti. I programmi di formazione devono essere progettati per arrivare al cuore della nostra società e dovrebbero diventare parte integrante del sistema educativo. I curricula non dovrebbero concentrarsi solo sulle capacità di programmazione o di conoscenza tecnica, ma anche sulle conoscenze di sicurezza: dobbiamo costruire un **lessico di sicurezza** e un **framework condiviso** per comprendere il comportamento nella sfera virtuale. E c'è ancora molto da fare.

Conclusioni

Peggy Ertmer sostiene che cambiare le abitudini è una cosa molto complessa, ma che può essere ottenuta attraverso l'esercizio, il supporto culturale e il cambiamento delle convinzioni all'interno della società. C'è ancora un lungo cammino da fare per arrivare a ottenere un ambiente cyber sicuro, come nel mito di Ercole e della virtù: stretto e pieno di ostacoli all'inizio, ma ampio e arioso alla fine. Nell'ambiente militare si dice che se vuoi la pace, devi preparare la guerra.

Quello che dobbiamo fare è considerare questo articolo e le idee qui contenute nella loro interezza. Se vogliamo cambiare la cultura della sicurezza nella nostra società, dobbiamo, come dice la D.ssa Mary Aiken, fermarci, disconnetterci e riflettere. Dobbiamo ricordare l'essere umano. ■

Enterprise e security: scegliere oggi la strategia per essere sicuri domani

Nelle smart city dispositivi e sensori interagiranno automaticamente con noi permettendo servizi personalizzati. Saremo sempre più integrati ai dispositivi che già ora indossiamo. Telefono e orologi possono certificare la nostra identità in base a caratteristiche biometriche avanzate, quali il modo di muoverci, e interagire automaticamente con altri dispositivi.

Autore: Alessandro Della Negra

Proteggere la nostra identità sarà fondamentale: anche l'uomo comune capirà l'importanza della CyberSecurity.

Ora siamo in una situazione di transizione in cui la CyberSecurity è chiaramente posta ai primi posti per importanza da parte della fascia di persone a cultura tecnologica più avanzata, ma i mezzi per capirne i principi non sono comunemente conosciuti. Spesso anche le aziende sembra si adeguino per motivi normativi più che per un reale convincimento che in un mondo sempre più virtuale solo la sicurezza Cyber può garantire l'essenza stessa del business.

Ma qual è la strategia migliore che dovrebbe adottare ora una azienda per la CyberSecurity? Analogamente, come massimizzare il ritorno a lungo tempo dall'investimento in CyberSecurity?

Questo va considerato in ambienti complessi in rapidissima evoluzione, con nuove minacce ora non prevedibili, legate agli strumenti e app che si utilizzeranno, con una difficoltà, per molti impossibilità, di essere aggiornati; con tempi dettati dal business, in cui i ritardi si possono pagare molto cari.

Viste queste caratteristiche la protezione, almeno operativamente, non potrà che essere sempre più affidata a partner specializzati affidabili o a servizi gestiti, che spazino dalla propria infrastruttura al cloud. Fondamentale avere processi e infrastruttura che permettano l'intercambiabilità del partner (o del proprio team) con impatti minimi.

Ma quanto mantenere in casa e che livello di controllo mantenere? Un punto importante: la strategia di protezione deve essere scelta dall'azienda in quanto un errore strategico nella security equivale a un errore simile nel proprio core business. Può portare l'azienda a diventare marginale.

Quali quindi le caratteristiche strategiche delle soluzioni di Cybersecurity da adottare?

Da un punto di vista infrastrutturale sicuramente è necessario puntare su automazione e semplificazione della gestione per ridurre al minimo la possibilità di errori. Quindi:

- Riduzione degli strumenti di gestione dell'infrastruttura di security;
- Riduzione dei dispositivi (sonde e attuatori) che interagiscono con la rete;
- Valutazione attenta dell'impatto operativo di ogni soluzione che si desidera inserire a protezione di specifiche funzioni.

Per capire il perché di questi punti pensiamo a come si è evoluta la CyberSecurity nel tempo. Inizialmente il firewall "stateful" dava tutta la protezione necessaria, poi le minacce si sono evolute e si sono create diverse soluzioni che controllavano maggiormente i dati in transito; quindi soluzioni di IPS, AV, Content filtering, URL filtering e quant'altro, con componenti dedicate e mancanza di interazione tra i diversi dispositivi con la complessità di gestione e mancanza di coordinazione tra l'intervento di queste diverse soluzioni (anche se magari sullo stesso device fisico).

Ora la situazione è analoga, i firewall fanno molto di più, capiscono le applicazioni e i dati, ma spesso le componenti che integrano non comunicano tra di loro. Inoltre nuove applicazioni e nuovi trend portano a nuove minacce e nuove soluzioni per fronteggiarle. Il cloud porta soluzioni

CASB, il fatto che ci possano essere utenti compromessi internamente a soluzioni di *behaviour analysis* e così via, con il moltiplicarsi di soluzioni "best of breed" che rispondono perfettamente all'esigenza puntuale ma che poi non sono realmente efficaci nell'integrarsi con il resto dell'infrastruttura.

Prendiamo l'esempio sopracitato di *behaviour analysis*. Una nuova soluzione allo stato dell'arte deve prevedere un certo numero di sonde per intercettare le attività degli utenti in rete, deve poi metterci l'intelligenza per analizzare questi dati ed infine, se si vuole automazione, le sonde devono anche poter bloccare il traffico. Rimane l'esigenza di integrazione con il resto dell'infrastruttura di security. Spesso questa funzione viene lasciata all'uomo che però è strutturalmente non adatto ai ritmi richiesti dall'automazione. Per questo è utile il supporto di strumenti di correlazione da configurare opportunamente.

Quante inutili duplicazioni per avere comunque il fattore umano come elemento limitante.

Il vero valore in questo caso sta nell'intelligenza artificiale dell'analisi dei dati. I dati potrebbero però provenire dalle sonde già in rete anche agenti sul traffico: gli attuali firewall. Inoltre l'ideale sarebbe inserire questa funzione in una piattaforma di security esistente in modo da avere una integrazione automatica.

Attualmente molte delle soluzioni di sicurezza "sprecano" nell'infrastruttura (sonde, memorie di massa, server, …) le risorse economiche necessarie ad implementarle, lasciando una parte minoritaria dell'investimento del cliente (e anche degli investimenti del produttore stesso) ad occuparsi del problema principale per cui vengono acquisite. Inoltre richiedono molte altre risorse per la gestione e per l'integrazione delle stesse con l'esistente.

Il mercato si sta evolvendo in tal senso. Come esempio possiamo considerare Palo Alto Networks, l'azienda che ha introdotto il concetto di Next Generation Firewall e che è un riferimento tra le aziende principali in questo settore. I tre passi evolutivi fondamentali della proposta sono stati:

- Introduzione del concetto di NGF, con firewall fisici e virtuali;
- Introduzione della platform, insieme di soluzioni completamente gestite in casa che integra in una soluzione omogenea e consistente tutte le componenti di network security (incluse quelle avanzate come la DNS security e il controllo degli zero day), le componenti di Cloud Security (via API e di controllo dell'infrastruttura), di End Point security, di behaviour analysis e di Threat Intelligence. L'interazione tra tutte queste componenti permette una risposta immediata e automatica a tutte le nuove minacce;
- Introduzione della possibilità per terze parti di sviluppare applicazioni di sicurezza per la propria piattaforma.

Proprio l'ultimo rappresenta un punto chiave nello sviluppo delle piattaforme di security: chiunque abbia nuovi algoritmi utili alla security di una singola azienda, di un intero settore o all'intero mercato non dovrà più preoccuparsi di costruire una infrastruttura e venderla al cliente per avere i dati su cui operare. Potrà sfruttare la piattaforma esistente e concentrarsi sulla propria soluzione di sicurezza addizionale.

Questo potrebbe portare nel mercato della security l'evoluzione che le app hanno portato agli smartphone. Forse prematuro dirlo ora, comunque sicuramente il fatto di avere una unica piattaforma con soluzioni allo stato dell'arte in ogni singolo componente è un fattore vincente. Fattore che però non può soddisfare tutte le esigenze degli utenti se non tramite lo sviluppo di app da parte di vendor più pronti nel fornire soluzioni specifiche. Vendor anche minori che, sfruttando la diffusione della piattaforma di Palo Alto Networks, possono affermarsi senza la necessità di grossi investimenti.

L'affermazione delle app di security rappresenta ancora una scommessa, ma sicuramente il concetto di platform rappresenta lo stato dell'arte nell'ottica di massimizzare il ritorno dagli investimenti in CyberSecurity.

Ritornando al tema: quanti tool di gestione sono necessari per una infrastruttura di security?

Non esiste una risposta. Molte cose sono inevitabilmente diversificate quindi difficilmente inglobabili. Tool di rete (switch, Wifi, accesso) e una soluzione di correlazione (che deve includere sorgenti completamente diverse) dovranno far parte della soluzione complessiva.

Restano molte altre soluzioni allo stato dell'arte non inglobate in una piattaforma che ad ora richiedono soluzioni puntuali. In futuro potrebbero essere semplicemente delle app.

Rimandiamo a futuri articoli un approfondimento su piattaforme nell'ottica della riduzione dei punti di management da integrare una strategia di security durevole. ■

BIO

Alessandro Della Negra è direttore vendite di Westcon Italia e Grecia. Laureato con lode in Scienze dell'Informazione a Udine inizia la carriera occupandosi dello sviluppo delle soluzioni di networking, di accesso a Internet e di Internet security presso un distributore locale. Affianca allo sviluppo commerciale l'attività presales e di training, docente per i training di networking avanzato per conto di Apple Computer.
La diffusione delle soluzioni proposte tramite la creazione di un canale distributivo di partner specializzati lo porta in breve tempo a gestire le linee principali per fatturato.
Ha un ruolo chiave nell'apertura della filiale italiana di Risc Technology, poi acquisita da Noxs e successivamente da Westcon. Assume prima un ruolo di business developer poi di direttore tecnico e quindi di responsabile della divisione di security. Dotato di forte background tecnico, nella sua vita professionale è stato istruttore certificato per molte soluzioni di networking e sicurezza, cosa che gli permette di avere un'ampia visione del mercato in cui opera.
Per ogni commento o suggerimento:
alessandro.della.negra@westcon.com
Per approfondimenti:

Realizzata per essere esposta nel 2013 all'ITU (l'Unione Internazionale delle Telecomunicazioni), premiata dall'ITU e quindi tradotta ed esposta consecutivamente in 28 città di Romania, Polonia e Svizzera, la mostra è stata tradotta in italiano per le Poste Italiane, col patrocinio della Polizia Nazionale. E stata presentata in anteprima nel 2016 presso la "MakerFaire – European Edition" di Roma (dove ha superato i 130.000 visitatori). In 30 pannelli, l'esposizione illustra l'evoluzione delle tecniche di comunicazione e di manipolazione delle informazioni dai tempi più antichi ai social media usati oggi da tutti. Consente senza essere moralizzatrice di educare giovani ed adulti ad una fruizione consapevole e protetta di Internet.
La mostra è integralmente visitabile sul sito del Distretto di Cyber Security delle Poste Italiane, dove l'esposizione reale è allestita in modo permanente:
https://www.distrettocybersecurity.it/mostra-2/

Una pubblicazione

AGORA get to know! *e*

web for business swiss webacademy

A cura del Global Cyber Security Center

Redazione:
Laurent Chrzanovski e Romulus Maier
(tutte le edizioni)
Per l'edizione del GCSEC:
Nicola Sotira, Elena Agresti

ISSN 2559 - 1797
ISSN-L 2559 - 1797

Indirizzi:
Bd. Dimitrie Cantemir nr. 12-14,
sc. D, et. 2, ap. 10, settore 4,
040234 Bucarest, Romania
Tel: 021-3309282
Fax 021-3309285

Viale Europa 175 - 00144 Roma, Italia
Tel: 06 59582272
info@gcsec.org

www.gcsec.org
www.cybersecuritytrends.ro
www.agora.ro
www.swissacademy.eu

web for your business
swiss webacademy

together with:

Ville de Porrentruy
Histoire Vie Nature Formation

Presents:

CYBERSECURITY SWITZERLAND CONGRESS

2nd Edition

Western European Public-Private Dialogue Platform

November 29-30, 2018, Porrentruy, Switzerland

www.cybersecurity-switzerland.ch

Under the aegis and with the support of:

ITU

Global Cyber Security Center

Gendarmerie nationale
Une force humaine

Région-IHEDN Franche-Comté

Centre de recherche de l'EOGN

ANCOM
Autoritatea Națională pentru Administrare și Reglementare în Comunicații

SRI Patria a priori
Serviciul Român de Informații

Cyberint
Centrul Național
Serviciul Român de Informații

République et Canton de Genève
Post tenebras lux

Police Genève

Université de Genève
Global Studies Institute

IATA

FIC 2018

CCI Territoire de Belfort

Vallée de l'Energie

I Vichinghi sono qui per proteggerci

Clavister é un'azienda di cybersecurity svedese, crede che un'efficace sicurezza di rete sia nell'interesse di tutti.

Con un approccio che abbraccia l'intero ecosistema, sia fisico sia virtuale, proteggiamo e garantiamo la continuità del business dei nostri clienti e facciamo in modo che possano beneficiare dei migliori strumenti di protezione contro le minacce in costante espansione ed evoluzione.

Possiamo aver scambiato le spade con il software, ma il nostro spirito vichingo é rimasto intatto: crediamo che la miglior difesa informatica sia un deciso attacco contro ogni minaccia alla sicurezza.

Maggiori informazioni su
www.clavister.com/Vichinghi

clavister
CONNECT . PROTECT

SECURITY BY SWEDEN