Cybersecurity Trends

Edizione italiana, N. 3 / 2019

COMPUTER EMERGENCY RESPONSE TEAM

INTERVISTE VIP:

Rahav SHALOM REVIVO
Brig. Gen. Anton ROG

GLOBAL CYBER SECURITY CENTER

ISSN 2559 - 1797 / ISSN-L 2559 - 1797

Folder centrale: Speciale CERT

Global Cyber Security is our mission

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

Indice

BE CERT

Autore: Nicola Sotira

In questi giorni il Governo italiano ha varato il decreto **"disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica".** Con questo dispositivo si crea un vero perimetro di sicurezza cibernetica, inoltre, il Governo si dota di strumenti normativi che gli permettono di intervenire in maniera tempestiva ed efficace in caso di minacce e pericoli per la sicurezza nazionale.

Il decreto va ad integrare la direttiva europea NIS (Network and Information Security) indirizzando le società fornitrici di servizi essenziali e gli OTT del mondo digitale. Inoltre, sarà successivamente varato un altro decreto che definirà i nomi delle aziende core per la sicurezza nazionale che saranno inserite nel perimetro e si aggiungeranno alle 465 già individuate dalla direttiva NIS. Inoltre, nel decreto si prevede che il presidente del Consiglio, su indicazioni del **Comitato interministeriale per la sicurezza della Repubblica**, abbia il potere, in caso di crisi, di intervenire e provvedere alla rimozione della minacce sia in modalità difensiva che offensiva.

In questo contesto, che mette al centro il tema della sicurezza cibernetica del paese e delle sue infrastrutture, il ruolo dei Computer Emergency Response Team (CERT) assume la sua centralità. Questa unità affonda le sue radici negli anni 90 quando, a seguito del malware di Morris, ci furono danni per circa 100 milioni di dollari ed il blocco di una parte consistente di computer connessi alla rete Internet. Proprio a seguito di questo evento il Governo americano decise di creare, presso la Carnegie Mellon University, il Computer Emergency Response Team ovvero il primo CERT della storia.

I CERT sono uno strumento fondamentale per la protezione delle infrastrutture critiche e delle organizzazioni che operano nei servizi essenziali, sono strutture che dispongono di capacità di rispondere, in maniera efficace, agli incidenti di sicurezza informatica. Proprio nella parola response si evince il core della attività del CERT, ovvero la risposta nel caso di incidente. Inoltre, proprio grazie alle capacità di queste strutture, questi soggetti devono agire, sempre di più, come promotori della consapevolezza sui temi di sicurezza e porsi come educatori in quest'area.

Il CERT, paragonabile in alcuni aspetti alle unità di pronto soccorso nel settore sanitario, deve non solo provvedere alla gestione degli incidenti, ma farsi carico di tutte le attività concernenti la sicurezza degli asset e dei processi che devono essere protetti, Deve essere parte attiva nei temi di prevenzione, anche alimentando la consapevolezza degli utenti e di tutti i suoi stakeholder.

Il ruolo di queste strutture, come sottolineato da direttive nazionali ed Europee è diventato fondamentale, in questo ecosistema digitale sempre più interconnesso. Il CERT è il punto di riferimento sui temi collaborazione, condivisione e scambio di informazioni, temi essenziali per garantire la resilienza del sistema digitale. ■

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.

Il Framework Nazionale per la Cybersecurity e la Data Protection e la sua applicazione nel settore finanziario

CIS SAPIENZA
CYBER INTELLIGENCE AND INFORMATION SECURITY

Autore: Leonardo Querzoni

Le *best practices* per la protezione dei sistemi, delle informazioni e dei processi informatizzati hanno negli ultimi 10 anni subito forti evoluzioni, in una continua rincorsa alla contemporanea evoluzione delle minacce. Queste ultime oggi sono incarnate da una platea di attori molto diversificata: dal semplice criminale informatico, ad organizzazioni profondamente strutturate in grado di accedere a budget quasi illimitati (si pensi alle *advanced persistent threat* che agiscono per conto di attori statuali). Tali organizzazioni agiscono all'interno di un mercato nascosto, e per molti aspetti illegale, dove tecnologie e competenze avanzatissime sono a disposizione del miglior offerente, per gli scopi che questo ritiene più opportuni.

La crescita di queste realtà ha causato negli ultimi 10 anni il continuo aumento della asimmetria tra chi attacca e chi si difende, tanto che oggi anche avversari dalle capacità non elevate sono in grado di provocare danni ingenti. Le cronache hanno recentemente riportato[1] numerosi casi di piccole città statunitensi i cui sistemi informatici sono stati "presi in ostaggio" da criminali che, con tecnologie non particolarmente avanzate (una variante dei ben noti *ransomware*), hanno interrotto l'erogazione di moltissimi servizi informatizzati delle municipalità colpite, improvvisamente riportando al medioevo informatico comunità che contano milioni di cittadini. Nonostante queste tipologie di attacchi siano oggi ben note, ed esistano tecnologie in grado di prevenirne, o almeno mitigarne efficacemente l'impatto, il loro contrasto richiede un livello di consapevolezza dei rischi e di preparazione a livello organizzativo che è purtroppo ancora assente in molte realtà.

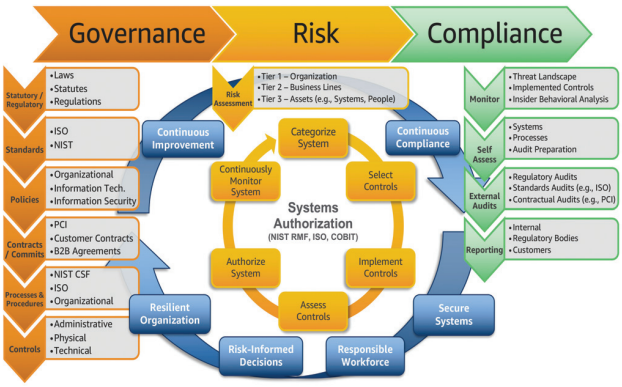
Ridurre l'asimmetria tra chi attacca e chi si difende è un processo che richiederà del tempo, e che inevitabilmente passerà attraverso ulteriori evoluzioni delle *best practice* di settore, ma quantomeno oggi la comunità che si occupa di sicurezza informatica è d'accordo sul fatto che sia necessario applicare una strategia ibrida fondata su tre pilastri fondamentali:

BIO

Leonardo Querzoni è ricercatore presso la Sapienza Università di Roma. I suoi interessi di ricerca spaziano dalla sicurezza informatica ai sistemi distribuiti con un particolare focus sull'affidabilità e la sicurezza dei sistemi complessi. È autore di più di 80 pubblicazioni su journal e in conferenze scientifiche internazionali. È inoltre co-autore del Framework Nazionale di Cyber Security, prodotto dal centro di ricerca in Cyber Intelligence and Information Security della Sapienza (CIS), di cui è membro.

la consapevolezza del rischio cyber, la protezione degli asset attraverso tecnologie avanzate ed una adeguata governance della sicurezza. Nessuno di questi tre pilastri, anche se sviluppato in modo avanzato, da solo può garantire un efficace contrasto alle odierne minacce; al contrario, solo una matura e bilanciata adozione di misure che coprano tutti e tre questi aspetti risulta sempre più spesso vincente.

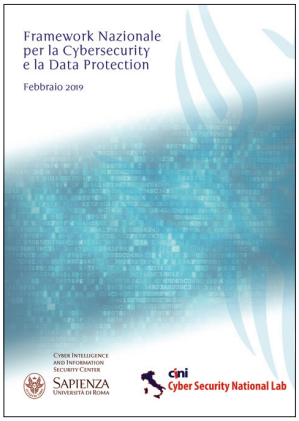
Governance della sicurezza



La governance della sicurezza[2] è un tema che, seppur non nuovo, sta oggi acquisendo sempre maggiore importanza a causa dell'allargamento della platea di organizzazioni che la adottano come parte della propria strategia di difesa cyber. In particolare, "governare la sicurezza" significa adottare tutte le misure necessarie a trasformare il problema della sicurezza degli asset informatizzati in un processo maturo, misurabile, ripetibile ed in grado di evolvere con le minacce.

In questo contesto la comunità internazionale ha sviluppato negli anni diversi *framework* che possono essere adottati come strumenti per l'implementazione di pratiche efficaci di governo della sicurezza. Tali framework hanno diversa natura; alcuni sono nati in ambito tecnico e propongono quindi soluzioni che al personale tecnico sono rivolte; altri adottano un approccio maggiormente gestionale delle problematiche di sicurezza, avendo quindi come target il management ed i processi organizzativi interni alle realtà che decidono di adottarli. Alcuni di questi framework sono certificabili attraverso più o meno complesse procedure di auditing; altri prevedono invece meccanismi di *self-assessment* non certificabili. Qualunque sia l'approccio utilizzato, tutti i framework condividono un unico obiettivo di alto livello: strutturare l'adozione e la gestione delle best practice di sicurezza attraverso un processo ben definito ed uniforme, potenzialmente condivisibile tra realtà che adottano gli stessi framework.

Il Framework Nazionale



Il Framework Nazionale per la Cybersecurity e la Data Protection[3], in particolare, rappresenta una soluzione pensata per adattarsi in modo duttile alle diversità del panorama italiano, costituito da realtà di diversa natura (es. pubbliche amministrazioni, imprese private, enti di diversa natura) e di diversa dimensione (dalle PMI alle grandi imprese).

Il Framework Nazionale nasce sulla base del NIST Cybersecurity Framework, ampiamente riconosciuto a livello internazionale, del quale eredita sia l'approccio basato sul rischio, che la struttura tecnica. All'interno del Framework Nazionale sono definite 117 attività abilitanti per la sicurezza, organizzate in cinque principali *function*: identify, protect, detect, respond, recover. Le cinque *function* coprono uno spettro estremamente ampio ed eterogeneo di attività che spaziano dai processi di gestione dei dati sensibili, alla protezione della supply chain. Per questo motivo, per essere applicato in modo efficace, il Framework Nazionale deve essere inizialmente contestualizzato al dominio in cui lo si vuole utilizzare.

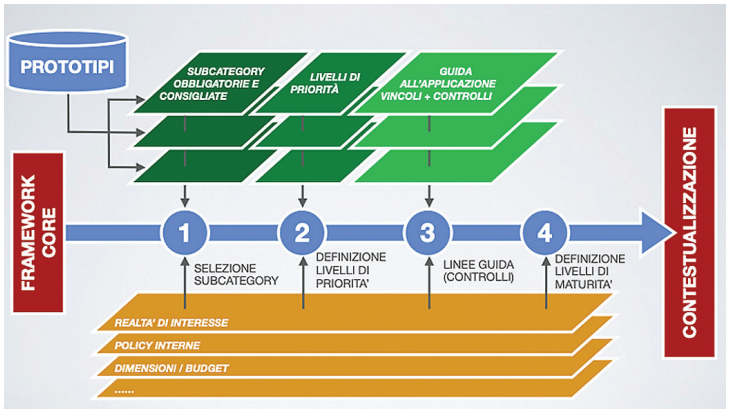


Figura 1: *Contestualizzazione del framework.*

Questa operazione di "contestualizzazione" (Figura 1) richiede di tenere in considerazione gli eventuali ulteriori vincoli che il dominio impone nella selezione delle singole attività abilitanti che nello stesso hanno senso. Ad esempio, per una azienda che eroga servizi software attraverso una piattaforma *cloud-based* gestita da un fornitore esterno, potrebbe non avere senso considerare un'attività legata all'uso di "meccanismi di controllo dell'integrità per verificare l'integrità del hardware" (attività identificata nel Framework Nazionale come PR.DS-8); d'altra parte la stessa attività è invece prioritaria per il fornitore della piattaforma *cloud-based* attraverso cui i servizi dell'azienda sono erogati.

Tra i vincoli più importanti che è necessario tenere in considerazione durante la fase di contestualizzazione del Framework Nazionale ci sono quelli legati alla *compliance* rispetto a regolamenti di settore, nazionali e non. Per facilitare questo aspetto, il Framework Nazionale si è recentemente dotato di uno strumento a supporto chiamato "prototipo di

contestualizzazione". Un prototipo rappresenta una selezione ragionata di attività abilitanti legata ad uno specifico regolamento o standard. In fase di contestualizzazione, diversi prototipi possono essere applicati al framework per identificare in modo semplice quali attività non dovranno essere escluse dalla contestualizzazione per supportare successivamente la *compliance* rispetto ai regolamenti di interesse. Il corretto uso dei prototipi semplifica fortemente l'attività di contestualizzazione del framework e fornisce la possibilità di definire un processo di contestualizzazione comune a tutte le realtà appartenenti a specifici settori regolamentati. Dato l'interesse e il vasto campo applicativo, il primo prototipo di contestualizzazione ad oggi offerto dal Framework Nazionale è quello relativo al GDPR. È stato inoltre pianificato lo sviluppo di ulteriori prototipi di interesse generale che saranno rilasciati tra la fine del 2019 e l'inizio del 2020.

Il Framework Nazionale per la Cybersecurity e la Data Protection è il frutto di una libera collaborazione tra organizzazioni private, pubblica amministrazione e centri di ricerca, con il supporto del Dipartimento Informazioni per la Sicurezza della Presidenza del Consiglio dei Ministri. Il mantenimento e l'evoluzione dello stesso sono curate dal Centro di Ricerca in Cyber Intelligence e Information Security (CIS) dell'Università degli Studi di Roma La Sapienza, in collaborazione con il Laboratorio Nazionale di Cyber security del CINI. Il Framework Nazionale e le risorse ad esso connesse sono liberamente disponibili alla pagina https://www.cybersecurityframework.it.

Il Framework Nazionale nel settore finanziario

Gli operatori del settore finanziario hanno storicamente sempre investito notevoli risorse sulla sicurezza informatica, mostrando una maturità nell'affrontare questo tema comune a poche altre realtà. Questo è probabilmente conseguenza del fatto che questo settore è stato tra i primi ad abbracciare negli anni '60-'80 la rivoluzione informatica, riuscendo quindi a coglierne le opportunità ma anche i rischi. Gli operatori finanziari stanno oggi mostrando un forte interesse nel Framework Nazionale, visto non tanto come strumento di elezione per implementare le proprie strategie di governance della sicurezza, già mature, ma piuttosto come strumento attraverso cui definire dei profili di sicurezza "target" condivisi e con cui auto-valutarsi rispetto a questi obiettivi.

In particolare, i ricercatori del CIS stanno oggi collaborando con diversi istituti bancari all'interno di un gruppo di lavoro il cui obiettivo finale è quello di costruire sul Framework Nazionale una metodologia di *assessment* che permetta a questi attori di confrontarsi e valutarsi volontariamente sulle strategie di sicurezza da loro adottate.

Per raggiungere questo obiettivo il gruppo sta oggi lavorando alla definizione di tutti i prototipi di contestualizzazione necessari per cogliere la specificità di questo settore, fortemente regolato. I prototipi che verranno prodotti terranno in considerazione normative di carattere generale (come la circolare 285 di Banca

d'Italia), normative inerenti servizi specifici (come la Direttiva (EU) 2015/2366 per i pagamenti) e normative trasversali che interessano potenzialmente anche alcuni soggetti del settore finanziario (come la Direttiva (UE) 2016/1148 sulla sicurezza delle reti e dei sistemi informativi). A valle di questa attività, ed entro la fine del 2019, il gruppo definirà una metodologia di assessment che usi il Framework Nazionale come suo cardine centrale.

Tutti i frutti di questa collaborazione, quando pronti, saranno liberamente distribuiti, proprio con l'intento di favorirne l'adozione da parte di tutta la comunità. ■

1 New York Times, "Ransomware Attacks Are Testing Resolve of Cities Across America", 2019 - https://www.nytimes.com/2019/08/22/us/ransomware-attacks-hacking.html
2 In questo articolo con il termine "sicurezza" si fa sempre riferimento alla sicurezza degli asset informatizzati.
3 Successivamente anche solo "Framework Nazionale".

Il sistema Cert Israeliano

Intervista VIP a Rahav Shalom Revivo, fondatrice del Cyber-Fintech Innovation Lab.

Rahav Shalom Revivo

Autore: Nicola Sotira

Nicola Sotira: Lo scenario Cyber è in continua crescita e le organizzazioni dovrebbero essere sempre più preparate ad affrontare nuove minacce. In questo contesto, qual è il ruolo di un moderno CERT, in particolare nel settore finanziario? Quali sono le priorità?

Rahav Shalom Revivo: In Israele, abbiamo un National Financial CERT che fa parte del CERT Nazionale Israeliano.

BIO

Rahav è Fintech e Cyber Innovations Manager presso il Ministero delle finanze israeliano con oltre 20 anni di esperienza nella R&D management, con particolare attenzione alle soluzioni Cyber, Fintech, DevOps e Cloud. Fa parte del Israeli National Financial CERT ed è la fondatrice del programma di laboratorio Fintech-Cyber Innovation - la prima iniziativa al mondo che sfrutta risorse e dati governativi per promuovere le startup Fintech e Cyber in una piattaforma di open-innovation. Rahav è stata nominata da lattice80 tra le prime 100 donne del settore Fintech nel 2019 e sta attualemte sta lavorando attivamente alla promozione delle donne nel settore tecnologico sia a livello nazionale che a livello municipale.

Il National Financial CERT ha la responsabilità di supportare la sicurezza informatica dell'ecosistema finanziario – attraverso attività di cyber threat intelligence a livello nazionale e internazionale, raccomandazioni su come mitigare le minacce e squadre di incident response che possono supportare sul campo le organizzazioni in un caso di bisogno.

Il focus del National Financial CERT è l'"end to end" dei processi finanziari identificati come fondamentali per il funzionamento dell'ecosistema finanziario, come il cash flow, le transazioni con carta di credito e molto altro. Lo stato e la resilienza dei processi finanziari determinano la definizione delle priorità e l'ecosistema finanziario stesso.

Nicola Sotira: Le attività preventive svolgono un ruolo importante. La condivisione delle informazioni potrebbe migliorare la resilienza dei servizi finanziari? Si sta lavorando in questa direzione?

Rahav Shalom Revivo: La chiave del successo è essere preparati a qualsiasi pericolo possa verificarsi. Pertanto, oltre alle esercitazioni sulla cybersecurity dedicate ai team specialistici che la cyber directorate sta conducendo, il Ministero delle Finanze sta promuovendo esercitazioni sulla resilienza informatica per la leadership finanziaria. Solo un anno e mezzo fa abbiamo svolto un'esercitazione a cui hanno partecipato il Ministero delle Finanze, il Central Bank Manager, tutti i regolatori finanziari e i rappresentanti del mercato privato, al fine di rispondere agli scenari drammatici che gli impatti di cyber attacchi possono avere sull'ecosistema finanziario e la conseguente necessità di adottare le necessarie decisioni finanziarie.

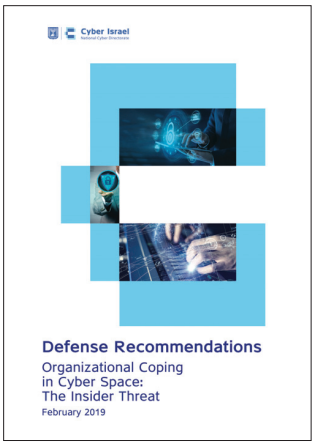
Inoltre, il CERT finanziario fornisce varie raccomandazioni agli istituti finanziari su come proteggersi. Le raccomandazioni variano dalla segnalazione di una specifica vulnerabilità, dominio o indirizzo IP da bloccare, all'identificazione di nuovi metodi di attacco, vettori, ecc.

Spetta agli stessi istituti finanziari decidere se seguire o meno una raccomandazione specifica. La cosa interessante dell'Israeli National Financial CERT è che non siamo un regolatore. Pertanto la collaborazione

delle istituzioni finanziarie con noi è completamente volontaria. Tuttavia, il 100% delle banche, il 100% delle Società di carte di credito e tutte le compagnie assicurative di grandi e medie dimensioni sono collegate al CERT finanziario per fruirne i servizi e segnalare gli incidenti.

Nicola Sotira: Il fattore umano si sta trasformando da punto vulnerabile alla prima linea di difesa contro gli attacchi informatici. Il tuo CERT sta investendo in awareness e formazione?

Rahav Shalom Revivo: È vero che uno dei collegamenti più deboli nella protezione della sicurezza informatica è il fattore umano. L'utente è ingannato e indotto a cliccare un collegamento o aprire un'e-mail malevola, collegare un USB non analizzato ma il rischio può essere rappresentato anche da un dipendente infelice che potrebbe diventare una minaccia interna.



L'Israeli National CERT sta lavorando direttamente con il pubblico, creando awareness.

Il CERT finanziario collabora direttamente con i CISO e i SOC. È responsabilità dei CISO educare e persino testare i propri dipendenti.

Mitighiamo il rischio da un'altra angolazione. Dal momento che ci concentriamo sui processi finanziari end-to-end, vogliamo assicurarci che ciascuno dei collegamenti in essi contenuti sia protetto e ciò significa che non solo gli istituti finanziari dovrebbero essere protetti ma anche i fornitori di terze parti che a loro volta fanno parte di questi processi. Questo è il motivo per cui abbiamo un'unità specifica del Ministero delle Finanze che si concentra sull'indirizzo della cybersecurity nella supply chain finanziaria e che sta lavorando con i fornitori più critici che sono coinvolti nei processi critici finanziari end-to-end, eseguendo survey sulla cybersecurity e fornendo loro raccomandazioni da seguire, al fine di assicurare la loro resilienza.

Ministry of Finance

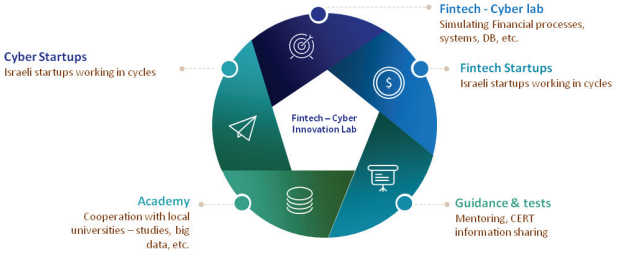
Cyber Security & Continuity Guidance Unit for the Financial Supply Chain

Nicola Sotira: Qual è il ruolo delle nuove tecnologie come l'intelligenza artificiale, il machine learning, la blockchain, il 5G? Questi strumenti possono davvero aiutare un CERT nelle sue attività tattiche operative strategiche?

Rahav Shalom Revivo: Il National CERT e il CERT finanziario stanno utilizzando nuove tecnologie come blockchain, AI e così via al fine di proteggere l'ecosistema finanziario e la sfera informatica israeliana in generale, sia attraverso prodotti "auto-sviluppati" che attraverso l'utilizzo di nuovi prodotti rilasciati.

Nicola Sotira: L'innovazione è ovunque. Come partecipate all'innovazione?

Rahav Shalom Revivo: In effetti, l'innovazione è ovunque, e come paese che regolarmente investe in essa, abbiamo voluto sfruttare i dati unici e le competenze che abbiamo al Financial CERT per promuovere fintech e cyber startup e aiutare Israele a diventare una nazione leader nelle fintech essendo già conosciuta come nazione cibernetica.



Ecco perché abbiamo lanciato il programma Fintech – Cyber Innovation lab. In questo laboratorio, destinato ai privati, vengono sfruttati dati governativi del settore cyber-finanziario per fintech e cyber startup in modo che queste possano sviluppare, testare e dimostrare i loro prodotti con una connessione ancor più forte alla sicurezza e agli eventi "live".

Siamo il primo paese al mondo che sta fornendo questi dati all'industria e tale attività è vista come una naturale evoluzione delle competenze che abbiamo acquisito.

Vogliamo che il settore privato possieda tali competenze per le proprie necessità e requisiti. Questo è il motivo per cui abbiamo pubblicato una gara che si chiuderà a metà novembre. Il laboratorio dovrebbe essere attivo e funzionante nel 2020.

CERT STAR

Nicola Sotira: Come migliorare la reale collaborazione tra le istituzioni finanziarie? GCSEC ha creato l'iniziativa CERT STAR, un programma di incontri tecnico-operativi dedicato agli analisti e agli operatori CERT per migliorare la loro collaborazione e competenze. Avete iniziative analoghe?

Rahav Shalom Revivo: Riteniamo che la condivisione delle informazioni sia uno degli strumenti chiave per diventare più resilienti. Questo è il motivo per cui l'Israeli National Financial CERT sta attivamente investendo in questo - oltre agli incontri periodici dei suoi membri, stiamo condividendo informazioni non solo con l'ecosistema finanziario locale (che sono i nostri clienti), ma anche con istituzioni finanziarie internazionali, come Poste Italiane. Tale collaborazione può fare la differenza: siamo molto più deboli come isole silos dove ognuna si prende cura solo del proprio territorio; gli attacchi informatici sono come onde di tsunami, danneggiano tutto ciò che incontrano sulla propria strada. Se resteremo uniti, ognuno di noi sarà protetto meglio. ■

Il CERT Finanziario Italiano

Autore: Mario Trinchera, coordinatore tecnico del CERTFin

Mai come in questo momento storico l'Unione Europea e i singoli Stati Membri impiegano risorse nell'aggiornamento o nell'introduzione di nuove norme (si pensi al CyberSecurityAct) e raccomandazioni in grado di rafforzare la protezione di dati, reti e informazioni, non solo attraverso nuove misure tecnologiche e di processo, ma anche attraverso l'incoraggiamento a costruire un vero e proprio governo nazionale di cybersecurity, con ruoli, responsabilità e architetture ben definite.

In questo contesto il mondo finanziario, da sempre tra i settori maggiormente presi di mira, segue con pari attenzione i cambiamenti tecnologici e di business, da un lato, e l'evoluzione del panorama delle minacce, dall'altro, per garantire un'offerta competitiva rispetto ad altri player, essere al passo con i tempi in relazione alle esigenze della clientela e mantenere livelli di sicurezza adeguati in termini di protezione non solo del denaro ma anche delle informazioni.

BIO

Laureato in Ingegneria Informatica presso l'Università di Napoli "Federico II", vanta una lunga esperienza nel settore della Difesa (Datamat, Selex, Finmeccanica, MBDA) ed ha conseguito diverse certificazioni internazionali in ambito security (tra cui la CISSP). Attualmente è il coordinatore tecnico del CERTFin, il CERT finanziario italiano: la mission del CERTFin è aumentare la cyber resilience dell'intero settore finanziario e le attività di cui si occupa spaziano dall'analisi su attacchi informatici e modelli di frode alla gestione delle emergenze derivanti da incidenti cyber. È coinvolto in vari progetti europei, finanziati dalla UE, ed è il PM del progetto REDFin che mira a realizzare una metodologia per la conduzione di cyber exercises basati su threat intelligence.
Partecipa a diversi tavoli internazionali (EBF, ENISA, FS-ISAC, SWIFT) ed è il coordinatore di diversi osservatori di ricerca (Cyber Security, Business Continuity, Artificial Intelligence) in seno ad ABI Lab, Centro di Ricerca e Innovazione per la Banca.

Nella complessa valutazione dei rischi cyber, guardare però soltanto al proprio perimetro aziendale non è più sufficiente: la sicurezza nel mondo cibernetico non ha confini, per cui il ridisegno degli scenari di rischio deve tenere conto dei nuovi attori dell'ecosistema digitale con cui ogni banca interagisce (come i provider di servizi e facility), spesso collocati anche al di fuori dei confini nazionali. La gestione del cosiddetto «third party risk» è infatti uno dei temi strategici su cui si potrà concentrare l'attenzione del mercato e dei regolatori nei prossimi mesi, con l'obiettivo di trovare modalità comuni di mitigazione e mantenere elevati i livelli di resilienza cyber dell'intero sistema.

Tuttavia, il vero fattore differenziante nella lotta al crimine informatico è rappresentato dalla capacità del settore di agire in maniera strutturata e coordinata, facendo tesoro non dell'esperienza limitata del singolo ma piuttosto dalla continua condivisione delle esperienze da parte di tutti. Su questa base, il 1° gennaio 2017, nasceva il **CERTFin** – CERT Finanziario Italiano: un'**iniziativa cooperativa pubblico-privata finalizzata a innalzare la capacità di gestione dei rischi cyber degli operatori bancari e finanziari e la *cyber resilience* dell'intero sistema finanziario italiano**.

Il CERTFin è co-governato dalla Banca d'Italia e dall' ABI che, attraverso un Comitato Strategico e un Comitato Direttivo ne indirizzano le attività. La **Direzione Operativa** è invece responsabile delle attività operative del CERT Finanziario e della gestione segretariale dei Comitati e amministrativa delle partecipazioni. Sotto il profilo operativo, è interessante notare che alcuni membri del CERT Finanziario contribuiscono con proprie risorse al funzionamento dello stesso, partecipando ad un **Team Virtuale**, secondo un modello organizzativo decentrato, denominato "campus".

La partecipazione al CERTFin è aperta, su base volontaria, a tutti gli operatori del settore bancario e finanziario nazionale, come: prestatori di servizi di pagamento, intermediari bancari e finanziari, imprese di assicurazione, gestori di infrastrutture di mercato, centri servizi e provider di servizi tecnologici rilevanti per il settore.

Il CERTFin ha diversi filoni operativi di cui è utile fare rapidamente una panoramica:

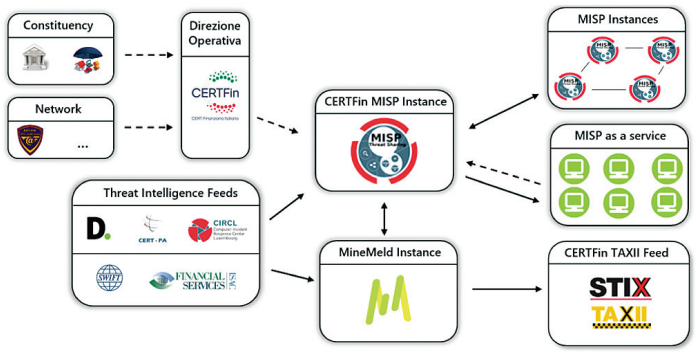
FINANCIAL INFO SHARING AND ANALYSIS CENTER (FinISAC)

È una della attività core, finalizzata a **facilitare lo scambio di informazioni** in maniera tempestiva circa potenziali *cyber-threatsper* il settore. Il CERTFin attinge da diverse fonti e riceve un'enorme mole di informazioni riguardanti attacchi cyber perpetrati in ogni angolo del mondo. Queste informazioni vengono filtrate in modo da selezionare solo gli "IOC" di interesse per il settore finanziario italiano e che sono indicativi di attacchi, magari anche avvenuti in un settore diverso, ma replicabili in quello finanziario.

La condivisione di queste informazioni avviene attraverso una *open platform* denominata MISP (malware info-sharingplatform) alla quale gli aderenti al CERTFin sono connessi e da cui riescono ad importare automaticamente tali informazioni nei loro rispettivi sistemi di difesa perimetrale.

Con dinamiche simili vengono condivisi anche codici IBAN coinvolti in attività fraudolente, azione questa che permette ai singoli istituti di bloccare tempestivamente transazioni da/verso i conti correnti associati.

Nell'arco di quasi tre anni, ovvero il periodo di operatività del CERTFin, sono stati analizzati oltre 1000 fenomeni, sono state pubblicate circa 1300 segnalazioni e sono stati raccolti circa di 5 milioni di IoC specifici per il settore finanziario.



L'architettura per l'information sharing tramite MISP

CYBER KNOWLEDGE AND SECURITY AWARENESS

Si tratta di un vero e proprio **osservatorio di ricerca** che approfondisce diverse tematiche, non necessariamente attinenti al solo mondo cyber. Sebbene tra le attività principali, ampio spazio sia dedicato all'analisi di minacce informatiche di ogni tipo e al monitoraggio continuo sull'evoluzione dei modelli di attacco, va anche sottolineato che i meeting periodici dell'osservatorio sono occasione di confronto su nuove minacce, su nuovi modelli di attacco, su nuove soluzioni tecnologiche ma anche su interpretazioni normative di cui il settore bancario deve confrontarsi costantemente.

Su richiesta dei partecipanti, vi è la possibilità di approfondire tematiche che indirettamente risultano essere connesse con i filoni di ricerca e spesso sono trattati da ospiti provenienti da settori diversi: ad esempio, recentemente il Poligrafico ha illustrato i dettagli e i requisiti di sicurezza del progetto sulla nuova Carta di Identità Elettronica, l'unità di crisi dell'Esercito che ha descritto i propri processi di *Crisis Communication Management*, fino ad un imminente coinvolgimento di un'azienda del settore del lusso che tratterà tempi relativi alla gestione delle terze parti.

> *Se tu hai una mela, e io ho una mela, e ce le scambiamo, allora tu ed io abbiamo sempre una mela ciascuno. Ma se tu hai un'idea, ed io ho un'idea, e ce le scambiamo, allora abbiamo entrambi due idee.*

L'infosharing secondo George Bernard Shaw

CENTRALE OPERATIVA DI GESTIONE DELLE EMERGENZE CYBER

Può capitare che un incidente di sicurezza colpisca un membro della Constituency; in questi casi il CERTFin fornisce supporto all'organizzazione colpita e facilita il processo di *resolution*, collabora con i singoli presidi di sicurezza, condivide le ***lesson learned*** al fine di prevenire ulteriori incidenti in altre organizzazioni. Ovviamente funge da punto di coordinamento centralizzato quando l'incidente è sistemico, cioè coinvolge più soggetti.

THREAT INTELLIGENCE AND LANDSCAPE SCENARIO

Il CERTFin, attraverso una propria piattaforma di Threat Intelligence, mira a prevenire l'insorgere di nuove minacce analizzando fonti aperte e fonti chiuse, nonché attingendo alla propria knowledge base. Il programma GTI (GenericThreat Intelligence) è finalizzato a produrre un *cyber-threat scenario* per il settore finanziario italiano, chiamato anche **GenericThreat Scenario** e che sarà pubblicato dal CERTFin con frequenza semestrale a partire dalla seconda metà del 2019. Lo scenario si concentra sull'identificazione delle minacce informatiche nazionali e settoriali e la sua realizzazione si basa sulla correlazione tra eventi malevoli, IoC, vulnerabilità e modelli di attacco.

AWARENESS

La protezione del cliente finale è considerata un punto chiave. Per questo motivo il CERTFin organizza periodicamente (con il supporto dell' ABI, della Banca d'Italia e della Polizia Postale) delle campagne di awareness rivolte al pubblico e specificatamente pensate per aumentare la consapevolezza di quanti utilizzano strumenti tecnologici potenzialmente esposti al rischio cyber e promuovere la cultura della security. Le campagne vengono veicolate attraverso noti siti web ma anche acquistando spazi dedicati su quotidiani nazionali di primaria rilevanza.

La campagna di awareness OcchioAlClic

Quest'anno la campagna, presentata al pubblico nel mese di maggio, durante il convegno Banche&Sicurezza, è stata denominata **"OcchioAlClic"** *(http://www.certfin.it/occhio-al-clic.html)* e ha l'obiettivo di fornire suggerimenti e consigli su come proteggersi dalle frodi ed utilizzare al meglio gli strumenti digitali.

ATTIVITA' INTERNAZIONALI

Infine, il CERTFin è fortemente coinvolto in numerose attività internazionali. Partecipa, infatti, stabilmente a 11 tavoli di lavoro (Europol, FS-ISAC, G7-CEG, EBFCSWG, Swift, etc…) ed attualmente partecipa attivamente a 3 progetti finanziati dalla Commissione Europea.

I progetti in questione trattano argomenti estremamente diversi, ed in particolare:

REDFin – Mira alla definizione di metodologie e modelli operativi per l'identificazione di scenari di minacce cyber e per la **preparazione ed esecuzione di test di tipo TableTop e RedTeaming**. Grazie alla consolidata collaborazione tra CERTFin e Banca d'Italia, i deliverable prodotti durante l'esecuzione del progetto ambiscono a contribuire alla definizione del nascente testing framework nazionale in ambito finanziario (TIBER IT).

CYBERSEC4EU – Il progetto, tra le cui finalità è prevista la realizzazione di un network europeo di centri di competenza cyber, non solo finanziari, coinvolge il CERTFin per la produzione di un **threat assessment sull'Open Banking**. Il compito sarà quello di affrontare le criticità di sicurezza associati all'entrata in vigore della PSD2, focalizzando l'attenzione sugli elementi tecnici e funzionali che sono collegati al paradigma Open API.

eIB – Il regolamento eIDAS (identificazione, autenticazione e firma digitale) fornisce una base normativa a livello UE per i servizi fiduciari e i mezzi di identificazione elettronica degli Stati membri.

Il progetto, sfruttando le peculiarità del Regolamento, mira a realizzare un processo di riconoscimento da remoto tra paesi membri che consenta agli utenti di interagire attraverso una **piattaforma e-marketplace** sviluppata ad hoc. Il CERTFin contribuirà a definire il processo nel settore bancario, svolgendo analisi tecniche e funzionali soprattutto in merito alle problematiche di sicurezza.

Nonostante le numerose e rilevanti attività già in corso, sono in programma ulteriori azioni per migliorare i servizi esistenti e crearne di nuovi, come ad esempio potenziare i flussi informativi verso la MISP, estendere le campagne di awareness anche ai canali televisivi, realizzare servizi dedicati al settore assicurativo.

Tutto ciò fa del CERTFin un caso praticamente isolato in Europa (esiste un Nordic Financial CERT ma con un set di attività molto più limitato) ed uno dei pochissimi al mondo. ■

Un numero verde per tutti i cittadini e le imprese, il nuovo risultato del CERT-RO

Autore: Cătălin Aramă

Dal 2 maggio, il CERT-RO ha lanciato il 1911, un numero di telefono verde gratuito 24 ore su 24, 7 giorni su 7, a disposizione di cittadini, imprese e istituzioni pubbliche in Romania. Grazie a questo numero, ogni vittima o presunta tale di un attacco di sicurezza informatica può denunciare l'incidente.

Questo risultato si traduce in una piattaforma di collaborazione tra operatori di servizi essenziali e fornitori di servizi digitali, che ha come obiettivo quello di contribuire all'educazione di coloro che sono coinvolti in incidenti di sicurezza informatica.

BIO

Cătălin Aramă è il direttore Generale del Romanian National Computer Emergency Response Team (CERT-RO). Con oltre 15 anni di esperienza nel settore IT, ha ricoperto posizioni di leadership sia nel settore pubblico che privato. È stato presidente del cluster IT «Dunărea de Jos» e responsabile del primo Software Park in Romania, nonché presidente del National Digital Romania Center, un'istituzione sotto il coordinamento del Ministero delle comunicazioni e dell'Information Society. Aramă è dottorando presso l'Accademia di polizia di Alexandru Ioan Cuza, Scuola di specializzazione per l'Ordine Pubblico e la Sicurezza Nazionale, e ha conseguito una laurea in diritto europeo e studi sulla pubblica amministrazione.

Il primo livello del Call Center è quello di fornire supporto, assistenza ed elaborare un triage. In questa prima fase viene fornito supporto tecnico alla vittima per far fronte in tempo reale all'emergenza, nonché assistenza per mitigare o risolvere l'incidente informatico. Internamente, contemporaneamente, viene avviato un triage, il che significa che all'evento viene dato un "Ticket" (numero unico con scheda contenente le caratteristiche specifiche dell'incidente).

Il secondo livello analizza le informazioni e, sulla base della diagnostica, il team CERT-RO contatta la vittima fornendo informazioni su come procedere in coordinamento con il team per affrontare l'incidente e, soprattutto, in questa fase l'evento si trasforma in un "cyber security alert", molto utile per coloro che potrebbero essere vittime dello stesso incidente. Creando il Call Center, CERT-RO ottempererà all'implementazione di tutti i requisiti imposti dalla direttiva NIS a tutti i CERT nazionali. In particolare consente di:

- creare un canale di comunicazione con persone, società private e le istituzioni pubbliche che sono sotto la responsabilità legale del CERT-RO, così come altre entità con le quali CERT-RO collabora, comprese le massime Autorità dello Stato;
- aumentare la disponibilità di tutti i servizi di comunicazione;
- collocare personale sufficiente per garantire il servizio 24/7;
- monitorare degli incidenti a livello nazionale in tempo reale.

Il successo del Servizio, misurato nei primi 5 giorni successivi al suo lancio, è impressionante: le chiamate ricevute hanno rivelato 87 alerts di sicurezza informatica unici, il 25% dei quali localizzati a Bucarest. Uno è stato segnalato da un ospedale i restanti dai cittadini.

Sostanzialmente gli incidenti unici giornalieri medi segnalati sono aumentati da tre incidenti al giorno (registrati per l'anno 2018, tramite il sito Web specifico) a 17 incidenti al giorno dopo il lancio del numero unico. A livello statistico, gli incidenti più segnalati, circa il 30%, appartenevano alla categoria della frode elettronica (phishing, estorsione, ecc.). I contenuti offensivi costituivano circa il 14% (spam, messaggi commerciali indesiderati, ecc.) e il resto degli alerts interessava sistemi compromessi (obsoleti, erroneamente configurati o non aggiornati di conseguenza), tentativi automatici di violazione delle password, di furto di informazioni, nonché un attacco di tipo ransomware (crittografia dei dati del disco). ■

Investiamo in conoscenza e in formazione se vogliamo riprenderci la rete

Intervista VIP a Francesco Corona.

Francesco Corona

Autore: Massimiliano Cannata

La *Link Campus University* di Roma è stata tra le prime istituzioni accademiche italiane a trattare argomenti cruciali nel settore della sicurezza nei suoi molteplici aspetti (geopolici, strategico - militari e di intelligence, cibernetici e sociali). Il progetto editoriale che ha portato alla pubblicazione del saggio di ***Arturo Di Corinto*** giornalista freelance ed esperto di Cyber Security, *"Riprendiamoci la rete!"* rientra in un ampio progetto di formazione e di sensibilizzazione rivolto soprattutto a quella generazione del "pollice", nata e cresciuta in ambienti in cui le tecnologie di uso quotidiano sono ormai diffuse. Siamo entrati nei contenuti del libro dialogando con Francesco Corona, che nell'ateneo romano, insegna *Cyber-Intelligence*.

BIO

Francesco Corona è docente e direttore del master di Hacking ed Ingegneria della Sicurezza presso Link Campus University Rome, già docente a contratto presso la Facoltà di ingegneria gestionale di Roma2 Tor Vergata Dipartimento di Ingegneria dell'Impresa. Ha svolto intensa attività di ricerca in ambito MIUR ed attività professionale d'impresa nel settore della sicurezza per conto di primari player nazionali ed internazionali. Nel 2013 consegue il prestigioso Premio Nazionale per l'innovazione e il premio ICT Confindustria. f.corona@unilink.it

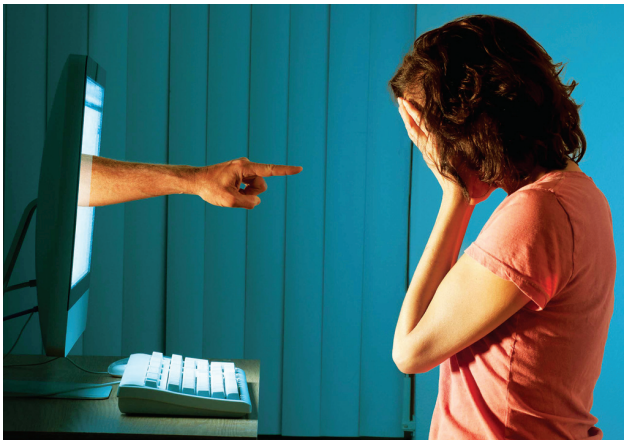
Professore: "Riprendiamoci la rete!" è un titolo che suona come un manifesto. Cosa sta avvenendo nel mondo di Internet?

La rete si sta trasformando da area della libera creatività a luogo denso di pericoli entro cui bisogna muoversi con cura. E' questo il passaggio di fondo che dobbiamo comprendere in questa fase di eccezionale sviluppo del digitale. Siamo tutti esposti a delle minacce che provengono non solo dagli strumenti che possiamo definire classici, quali i virus e i *malware*, ma anche dagli *APT* (*advanced persistent threat*, attacchi mirati e persistenti n.d.r) che mettono sempre più a repentaglio l'integrità delle reti e dei sistemi telematici. Siamo di fronte a un alto livello elevato di esposizione, che riguarda in modo particolare i *social*. Sulle infrastrutture informatiche dati personali e dati sensibili, di cui non riusciamo a seguire il percorso a dispetto

delle tante policy e delle normative che dovrebbero garantire un controllo severo sulla loro utilizzazione. Ma i pericoli non finiscono qui…

A cosa si riferisce in particolare?

Fenomeni sempre più diffusi di *cyber* bullismo rendono il quadro ancora più inquietante. Le categorie più esposte sono proprio quelle dei giovani. I nativi digitali crescono "immersi" nella dimensione del digitale non rendendosi conto dei rischi che corrono.

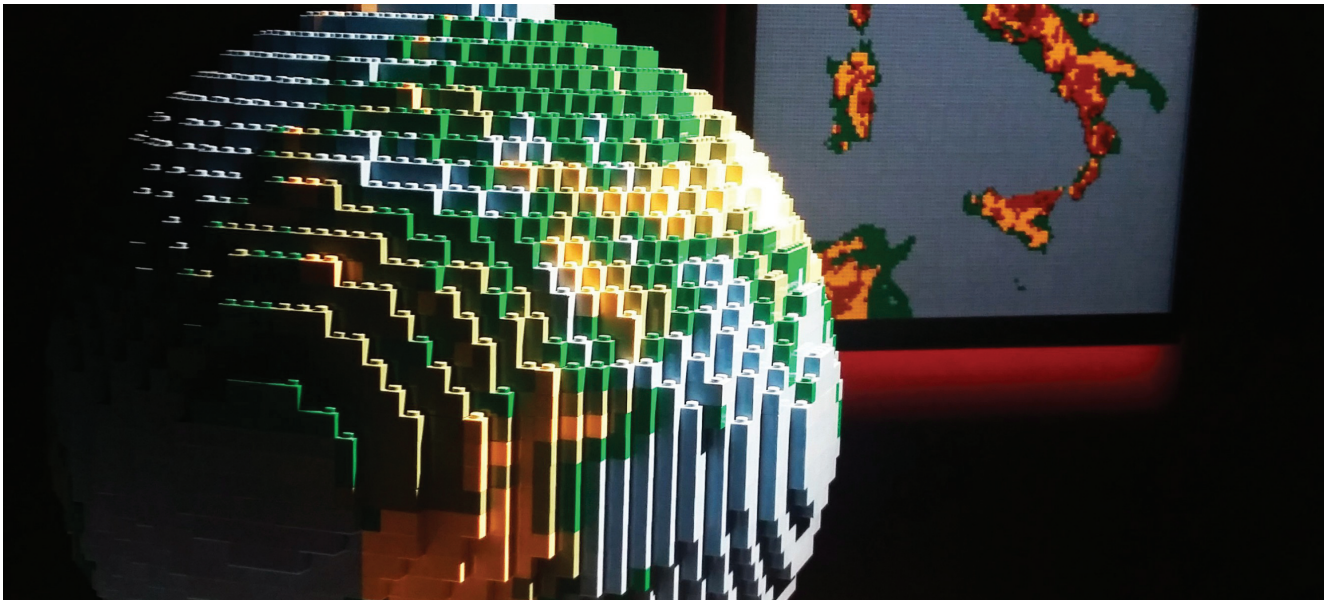


Acquisire consapevolezza del pericolo è il primo messaggio chiave della pubblicazione che si caratterizza per un impianto innovativo. Le ragioni del successo e dell'interesse che sta suscitando risiedono nella modalità con cui sono organizzati i contenuti?

Il manuale è strutturato con delle schede informative arricchite da immagini molto esemplificative, il linguaggio è molto asciutto, chiaro, diretto. Sto tratteggiando quelle che sono prerogative dell'autore, docente della Link Campus e grande conoscitore della materia. Di Corinto ha, in particolare, la capacità di far emergere quelle vulnerabilità che a un occhio superficiale di solito sfuggono, rimanendo sotto traccia.

A giudicare dai rischi che si corrono bel illustrati nella trattazione, per chi è abituato a relazionarsi "on life" (per usare una fortunata definizione di Luciano Floridi), e per chi abita quotidianamente i social, è dura, non crede?

Non credo sia così a patto di saper mettere in campo un doppio livello di intervento: da un lato gli esperti che devono con tempestività individuare le problematiche e le criticità che attengono alla sicurezza informatica, dall'altro i comunicatori, che hanno il compito di trasmettere le problematiche al grande pubblico, fatto di target differenti, tutti da raggiungere in maniera pertinente ed efficace. La rete non è solo frequentata dai ragazzi, ma come è noto anche da persone senior che utilizzano gli strumenti del digitale per soddisfare molteplici interessi. Queste categorie hanno in comune un aspetto: affrontano entrambe la rete in modo sprovveduto e inconsapevole.



L'Università che compito deve svolgere in questo delicato "cambiamento d'epoca"?

La *Link University* sta investendo molto sul versante della formazione e della sensibilizzazione. Dirigo il Master in *Ingegneria della sicurezza* e sono codirettore del Master in *Cyber Security*. Inoltre ci stiamo occupando di far conoscere alle giovani generazioni le contromisure adeguate per difendere i sistemi telematici e cibernetici da attacchi sempre più sofisticati.

Un impegno a largo spettro quello che la Link ha messo sul tappeto che coglie giovani con un livello di studi ed esperienze, le più variegate. Non deve essere facile trovare linguaggi e metodi in comune?

E' complesso, ma importante che sia così. Sono responsabile del nodo *CyberChallenge* della *Link Campus University*. In questo ambito illustriamo ai ragazzi il nuovo programma del laboratorio nazionale di Cyber security. Si tratta di un lavoro tecnico - scientifico che viene presentato con il linguaggio del gioco e nelle sembianze della simulazione. Occorre anche aggiungere che, per chi ha già una certa esperienza, frequentare questi corsi significa acquisire conoscenze fondamentali per l'autodifesa.

Veniamo ora al secondo termine chiave: l'autodifesa. Come va interpretata?

Nell'accezione più ampia, perché la mappatura del rischio riguarda oggi imprese, istituzioni, ambienti

cini
Cybersecurity
National Lab

sanitari, scuole, infrastrutture critiche, senza dimenticare i pericoli insiti nelle mura domestiche. I ragazzi che seguono i nostri corsi sono capaci di predisporre sistemi di difesa avanzata per organizzazioni produttive che operano in tutti questi delicati ambiti.

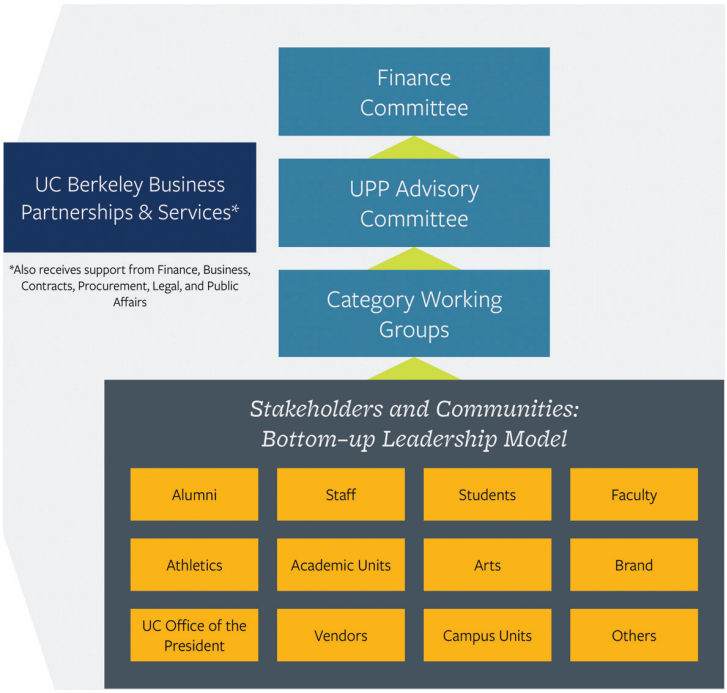
Chi non ha delle attitudini per i temi della sicurezza, è destinato a "segnare il passo" in questo orizzonte in cui diventano sempre più importanti le competenze hi-tech?

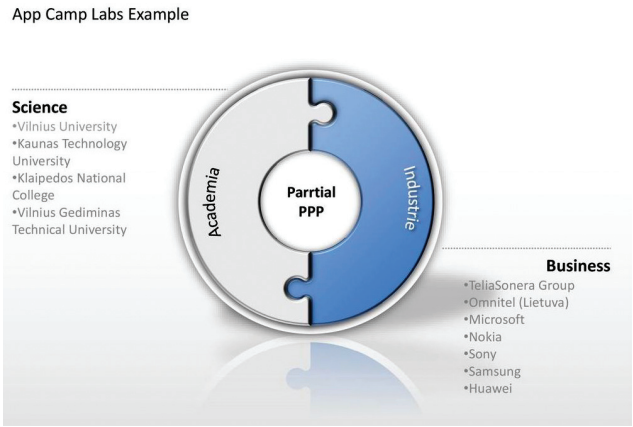
Tutt'altro. I giovani che non hanno un interesse specifico, devono essere portati a un livello di consapevolezza necessario utilizzando tutti gli strumenti per una divulgazione efficace. Ho partecipato al Cybertech, che si è tenuto presso *La Nuvola* di Roma poche settimane fa. Molte aziende stanno proponendo dei giochi di gruppo per addestrare i giovani alla

sicurezza. Sono iniziative molto importanti proprio perché non riguardano la stretta cerchia degli addetti e aiutano a creare i presupposti per una consapevolezza diffusa del valore strategico della sicurezza. Innalzare i livello di percezione del rischio, è il filo rosso che lega tutte le attività formative che stiamo portando avanti nella nostra Università, di cui il libro del collega Di Corinto è un tassello fondamentale.

Vorrei che si soffermasse su un ultimo aspetto: il livello di collaborazione tra Università e impresa. A che punto siamo su questo delicato terreno?

La collaborazione tra queste realtà deve essere rafforzata. Fino ad oggi lo scambio è stato sostanzialmente dettato dall'analisi di curricula che vengono messi dall'Università a disposizione delle aziende per avviare degli stage propedeutici all'inserimento nel mondo del lavoro dei giovani. Bisogna fare di più; andare oltre il semplice intervento di *sponsorship* da parte delle grandi imprese su eventi e iniziative spot. Deve farsi strada un impegno strutturale e una messa a bilancio di budget finalizzati allo sviluppo della cyber security. Bisogna insomma impegnarsi per rendere strutturale, la collaborazione tra Università e aziende, definendo precisi obiettivi formativi orientati a colmare il deficit di figure professionali che il mercato richiede nel settore della cyber security. Da un'azione mirata ed efficace ne guadagnerebbero tutti: le imprese perché acquisirebbero figure preparate, sensibili e consapevoli, e la società nel suo complesso perché questo "salto" di metodo e di visione avrebbe riflessi importanti sul piano occupazionale, con conseguenze positive per l'intero sistema - paese. ■





Le basi delle PPP University - Business della Berkeley University ed il modulo "cyber" delle Università della Lituania

Sfide e priorità in ambito Cyber Security

Autore: Francesco Corona

Parlando di sicurezza delle reti e delle infrastrutture primarie, la parola chiave che ora più che mai può essere associata a quella di **Cyber Security** è certamente quella di **Sicurezza Nazionale**.

Come premessa fondamentale ed orientativa, possiamo dire che il primo atto del nuovo governo Conte bis va proprio in questa direzione e sottolinea l'importanza attribuita agli scenari attuativi del decreto Golden Power. Esercitando i poteri speciali nei confronti di società connesse alle forniture di sistemi di telecomunicazione 5G ed in particolare a quelle cinesi, il nuovo governo ha posto in essere un primo atto di importanza strategica per la sicurezza nazionale ed europea.

BIO

Francesco Corona è docente e direttore del master di Hacking ed Ingegneria della Sicurezza presso Link Campus University Rome, già docente a contratto presso la Facoltà di ingegneria gestionale di Roma2 Tor Vergata Dipartimento di Ingegneria dell'Impresa. Ha svolto intensa attività di ricerca in ambito MIUR ed attività professionale d'impresa nel settore della sicurezza per conto di primari player nazionali ed internazionali. Nel 2013 consegue il prestigioso Premio Nazionale per l'innovazione e il premio ICT Confindustria. f.corona@unilink.it

In Italia gli indicatori mostrano un buon trend attuativo della normativa europea NIS (Network Information Security) attraverso il DECRETO LEGISLATIVO 18 maggio 2018, n. 65 (in attuazione della direttiva UE 2016/1148) affiancato da un primo modello nazionale di Framework per la CyberSecurity basato su specifiche americane NIST e l'implementazione del nuovo regolamento europeo per la protezione dei dati personali (GDPR). La normativa NIS nella sua applicabilità alle infrastrutture critiche vede attualmente l'individuazione di Operatori di Servizi Essenziali e Fornitori di Servizi Digitali sottoposti al coordinamento del DIS (Dipartimento Informazioni per la Sicurezza) riguardanti "le più significative attività di approntamento del sistema di difesa cibernetica, tra cui il perimetro di copertura degli assetti di difesa comuni tramite i CERT/CSIRT, la certificazione di soluzioni SW/HW tramite laboratori qualificati, l'identificazione delle funzioni manageriali/professionali critiche, l'obbligo di condivisione degli eventi cibernetici significativi" (Information Sharing).

SISTEMA DI INFORMAZIONE PER LA SICUREZZA DELLA REPUBBLICA
a protezione degli interessi politici, militari, economici, scientifici ed industriali dell'Italia

Esistono tuttavia alcuni livelli di criticità da risolvere, prima di tutto la continuità attuativa messa in discussione dalle differenti crisi di governo. In secondo luogo, ma non meno importante, il mancato impiego di risorse economiche nazionali come *incipit* alla ripresa economica. L'Italia nel contesto europeo rappresenta una eccellenza sotto tutti i punti di vista. Nei settori strategici legati all'innovazione tecnologica, alla ricerca e alla sicurezza nazionale di cui quella cyber è certamente emergente, occorre una "Vision Strategico-Attuativa di un Sistema Paese moderno" che deve necessariamente puntare su livelli di formazione avanzati valorizzando le eccellenze emergenti nel dominio delle nuove capacità delle generazioni di giovani impegnate in studi scientifici interdisciplinari con particolare riferimento alle scienze dell'informazione e cybersecurity. Tutto ciò necessita di investimenti concreti e non solo dichiarazioni di merito a soli fini politici.

Un primo passo verso questo modello è stato fatto con i programmi della Cyber Challenge organizzati dal CINI (https://cyberchallenge.it) in collaborazione con alcune Università-Nodo (attualmente 18) ed alcuni istituti superiori afferenti a tali nodi con risorse economiche provenienti per lo più da sponsorizzazioni private, mentre il programma dovrebbe trasformarsi in un vero e proprio Piano Addestrativo Nazionale con finanziamenti pubblici strutturati e risorse da investire in poligoni addestrativi e simulativi (Cyber Range) da utilizzare in tutte le scuole ed università italiane.

Da questo punto di vista il cosiddetto "Piano Nazionale Scuola Digitale" non sembra idoneo a coprire le reali esigenze di sviluppo del Sistema Paese e della domanda di specialisti cyber da parte delle imprese nazionali ed europee, d'altra parte il neonato Ministero "senza portafoglio" dell'Innovazione Tecnologica e Digitalizzazione affidato alla torinese Paola Pisano dovrà certamente procurarsi risorse straordinarie per ottemperare alle emergenti sfide imposte dalla reali esigenze di innovazione *made in Italy*, probabilmente ricorrendo non solo a fondi speciali (di difficile reperimento europeo) ma come ipotesi concreta a un nuovo disegno di rivalutazione economica scritturale inteso come misura del valore indotto dai **nuovi assets economico-strategici per la sicurezza nazionale**, ridefiniti proprio sui settori tecnologici emergenti come le infrastrutture critiche nazionali o questa nuova tipologia di poligoni di addestramento. Tali operazioni rivalutative, da attuare con estrema urgenza, ricordano quanto fu fatto negli anni ottanta dal ministro Andreatta con l'approvazione della normativa sul Franco Oro per la valutazioni economico scritturale di infrastrutture di telecomunicazione nazionali in particolari Aree Strategiche di Affari.

CYBER CHALLENGE
CyberChallenge.IT

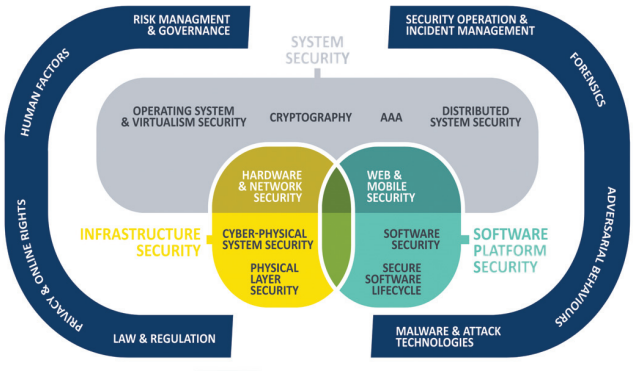
Oggi con le esigenze della Golden Power potrebbe profilarsi una situazione analoga a quella gestita negli anni ottanta dal governo italiano. In questi scenari di sviluppo dove si deve sottostare alle stringenti regole europee e ai diktat della BCE, e nello stesso tempo agli attacchi organizzati di gruppi hacker filo governativi di altre potenze economiche emergenti, la mossa di aumentare il gettito fiscale con l'aumento dell'IVA non sembra essere la più idonea per la stabilità di governo e per la competitività delle aziende. Occorre implementare meccanismi di rivalutazione ponderata degli asset strategici nazionali con opportune misure economico-strutturali che potrebbero rappresentare la vera soluzione vincente rispetto alla situazione attuale di stallo imposta dall'Europa.

Uno degli asset strategici sui quali puntare è riferito al concetto di "Awareness". Colmare il cosiddetto Cyber Security Skill Shortage (CSSS) potrebbe essere una postura fondamentale per l'Italia e per questo neo governo. Il modello inglese, con stanziamenti pubblici strutturali, potrebbe rappresentare una valida fonte di ispirazione. Tra il 2011 e il 2016, il Regno Unito ha investito ad esempio ben 32,8 milioni di sterline per i programmi di formazione ed educazione in CyberSecurity; il nuovo Cyber Discovery Program è stato creato per innovare i processi di formazione degli studenti nelle materie di Cyber Security e con il risultato che ben 23.000 studenti hanno aderito rispetto alle poche migliaia dei programmi di Cyber Challenge italiani che come dicevamo vengono finanziati dalle sole sponsorizzazioni di aziende private.

Le piattaforme di addestramento avanzato riguarderanno in primis i seguenti contenuti formativi:

- Studio olistico alla protezione di infrastrutture critiche, analisi dei rischi e valutazione e mitigazione del danno;
- Identificazione di vulnerabilità in ambienti complessi cyber fisici, learning machine e data mining;
- Threat intelligence avanzata, studio ed utilizzo di una piattaforma di arricchimento semantico dei dai rilevati;
- Realizzazione dinamica di framework per il monitoraggio e l'analisi del comportamento di sistemi complessi per l'identificazione di vulnerabilità e possibili percorsi di attacco;
- Nuovi e sempre aggiornati simulatori di Cyber Challenge e Cyber Range con analisi delle cosiddette "Kill Chain";
- Malware Analysis e reporting forense con uno studio di una suite di strumenti finalizzati all'analisi automatizzata dei sistemi oggetto di attacco;
- Crittografia e crittografia quantistica.

Tutto ciò necessita la creazione di un partenariato tra governo, industria e sistema educativo per ideare una soluzione nazionale al CSSS inclusiva di tavoli progettuali estesi al MIUR al MISE e al neonato Ministero dell'Innovazione Tecnologica e Digitalizzazione. Successivamente progettare e finanziare le infrastrutture di addestramento. In Italia alcune università ed enti pubblici sono attualmente coinvolti in due programmi di ricerca Horizon 2020, stiamo parlando di SPARTA ed ECHO ma questi finanziamenti europei per i quali l'Italia gestirà una aliquota intorno al 30% circa su 32MLN di Euro complessivi stanziati, sono ben poca cosa rispetto a quanto deve essere fatto con urgenza a tutela della sicurezza del nostro paese. Gli scenari di utilizzo delle nuove professionalità emergenti nella sicurezza cyber sono raffigurate nelle schema seguente:



Aree di richiesta di nuove professionalità nel settore CyberSecurity
Fonte: GCSEC "Mind the Gap" – 2019, Studio condotto da GCSEC con l'Università di Oxford ■

Percorso CyberChallenge Link Campus University

Intervista a Pierfrancesco Conti

Pierfrancesco Conti

BIO

Pierfrancesco Conti è uno studente iscritto al secondo anno di laurea magistrale in Cybersecurity presso l'università La Sapienza di Roma.
Nato ad Avezzano il 19 Marzo 1997, cresciuto a Roma, dove ha portato avanti gli studi fino a diplomarsi nel liceo scientifico Tullio Levi Civita. Sin dagli anni delle superiori ha coltivato la sua passione per l'informatica che lo avrebbe portato a laurearsi in Ingegneria Informatica ed Automatica all'età di 21 anni presso l'università La Sapienza di Roma. La scelta per la laurea magistrale è stata abbastanza ovvia: Cybersecurity. Questo perché da subito è rimasto affascinato dal tema della sicurezza in ambito informatico, dalla protezione di dati sensibili e da quei giochi chiamati CTF (Capture The Flag). Pierfrancesco così ha deciso di mettersi alla prova, iscrivendosi alla terza edizione della CyberCallenge.it 2019. La CyberChallenge.it è una competizione aperta a molte università italiane, tra cui la Link Campus University, il nodo per cui ha gareggiato, in cui gli è stato affibbiato dal celeberrimo prof. Francesco Corona lo pseudonimo di "Salom". Il suo obiettivo è quello di trasformare questi giochi nella sua occupazione professionale.

Autore: Elena Mena Agresti

La cybersecurity sta avendo un ruolo sempre più importante nel panorama internazionale. Ogni giorno si susseguono incessantemente attacchi informatici. Preparare i nuovi studenti a fronteggiare le minacce sembrerebbe, a detta di molti esperti, essere lo strumento migliore poter difendere al meglio il sistema paese. CyberChallenge.it nasce da una iniziativa del Laboratorio Nazionale di Cybersecurity del CINI il Consorzio Interuniversitario Nazionale per l'Informatica con l'obiettivo di addestrare alla cybersecurity i giovani delle scuole superiori e delle università. Quali sono state le fasi iniziali che prevedeva la competizione?

La competizione prevedeva due fasi iniziali che erano propedeutiche all'accesso alle fasi successive. Una prima che comprendeva un test di ingresso iniziale e che rappresentava il primo metodo di selezione composto da più fasi, utili per verificare capacità logiche e di programmazione e per determinare i 20 ragazzi che avrebbero partecipato al corso nei vari atenei. Esso era strutturato in due sotto fasi distinte. Un Pretest Online che consisteva in un quiz in inglese con domande di logica e di programmazione in "C" della durata di 60'. Un altro che invece prevedeva esercizi di problem solving di programmazione di vario genere dalla durata di 3 ore, utilizzando il linguaggio C, obbligatorio per uno degli esercizi assegnati, mentre per gli altri due era possibile scegliere le programmazioni C, C++, Python, Java, Scala etc.

CyberChallenge prevedeva oltre agli esami hands-on di cui ci hai appena parlato anche corsi di formazione. Quali sono stati gli argomenti trattati e qual è stato il valore aggiunto?

Lo scopo del corso CyberChallenge.it è stato formare giovani liceali o universitari nel campo della Cybersecurity, attraverso lezioni teoriche, riguardanti i vari temi della sicurezza, e lezioni pratiche, in cui ci si addestra a risolvere le *"Capture The Flag"*. Gli argomenti delle lezioni erano vari: dalla crittografia al reverse engineering, dai vari hacking tools alle infrastrutture di difesa. Ciò mi ha permesso di allargare le mie conoscenze in questo campo.

Durante i giorni del corso ho avuto modo di conoscere gli altri ragazzi che, come me, si trovavano in un ambiente nuovo. Molto velocemente è nata amicizia con chi fosse più simile a me in età ed interessi, ma man mano sono riuscito a conoscere ognuno di loro. Ci sono stati attribuiti dai nostri professori, prof. Corona (KETER) e prof. Gugliuzza (CEFEO), dei nicknames che ci avrebbero caratterizzato durante tutto il percorso.

Il corso era finalizzato a preparare i ragazzi a partecipare alle due gare previste, organizzate da CyberChallenge.it: la prima, di tipo Jeopardy, si è svolta localmente nelle sedi in cui ogni ragazzo ha seguito il corso ed è servita per determinare i quattro più idonei a partecipare alla seconda, di tipo Attacco-Difesa, in rappresentanza del proprio nodo.

In una gara di tipo Jeopardy più partecipanti devono risolvere le stesse sfide separatamente e senza interagire (anche situati in luoghi diversi). Nel nostro caso ogni nodo ospitava i suoi 20 (o meno) partecipanti in un ambiente favorevole a questo tipo di competizione (i.e. un laboratorio informatico) e si manteneva una scoreboard complessiva. Scadute le 7 ore fornite, sono stati definiti, ed in seguito premiati, i primi quattro partecipanti nella scoreboard per ogni nodo locale.

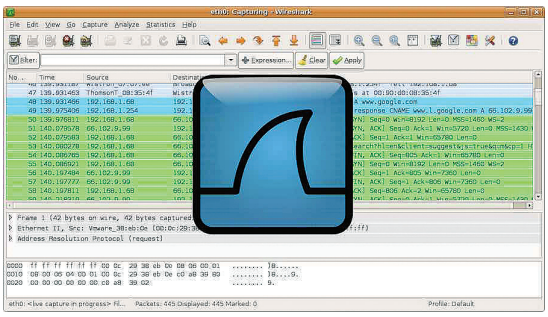
Conclusa la fase di formazione e competizione dei vari nodi a livello locale, sono state organizzate le Finali Nazionali congiuntamente dal Laboratorio Nazionale Cybersecurity CINI e dalla Scuola Telecomunicazioni Forze Armate (STELMILIT). Raccontaci come è andata e come si è svolta questa competizione finale.

Quest'anno la gara nazionale si è svolta nella caserma STELMILIT di Chiavari, dove i militari, gentilmente, ci hanno accolti in modo caloroso. Durante il viaggio ho avuto modo di stringere amicizia con i miei compagni ed i miei professori e di conoscerli meglio.

Nelle gare di tipo Attacco-Difesa, ai vari team vengono assegnate macchine identiche, le quali vulnerabilità possono essere sfruttate per attaccare quelle dei team avversari, ma possono anche essere corrette per difendere la propria. Nel nostro caso, per fare ciò, abbiamo potuto portare un raspberry PI e diversi tools sviluppati da noi per l'occasione.

Proprio in merito ai tool allora abbiamo utilizzato un automatizzatore per la sottomissione delle Flag quindi una volta che la squadra catturava una FLAG grazie ad uno specifico script utilizzavamo questo tool che ci consentiva di catturare più Flag insieme così da poter velocizzare tutti i processi essendo questa una gara a tempo. Poi abbiamo creato uno sniffer proxy che rappresenta un tool molto utile nel momento in cui qualcuno ci si trova sotto attacco e che consente di poter rovesciare l'attacco verso chi lo ha sferrato o per risolvere le nostre vulnerabilità o addirittura rivolgerlo anche ad altre squadre. L'importanza di analizzare il traffico è stata fondamentale. Per questa attività abbiamo utilizzato Wireshark, uno sniffer che consente di catturare pacchetti di rete e analizzarli di volta in volta ma lo strumento fondamentale durante la competizione è stato il gioco di squadra.

Risolvere le CTF infatti è una vera e propria collaborazione del team, proprio come abbiamo fatto durante l'anno (di lezioni n.d.r.) e essendo una squadra diversificata siamo riusciti a sfruttare le nostre capacità elemento fondamentale magari rispetto ai tool. Eravamo un gruppo versatile e questo ci ha aiutato ad affrontare le diverse CTF consentendoci di poter ragionare sulle modalità con le quali affrontarle.



La competizione ha avuto una durata di 7 ore e ciò è bastato a malapena per risolvere tutte le CTF che ci erano state proposte.

Cosa hai appreso e quale valore aggiunto ha avuto per te il CyberChallenge?

Questo percorso è stato fondamentale per lo sviluppo delle mie capacità e delle mie conoscenze nel campo della cybersecurity e senza dubbio è stata un'esperienza che mi ha arricchito e mi ha fatto crescere. Consiglio ai giovani di partecipare e di provare con tutte le forze a superare ogni prova che questa competizione possa presentare loro. Inoltre spero di essere utile ai prossimi partecipanti, fornendo consigli e conoscenze per la loro preparazione ed in vista delle gare.

Che consigli puoi dare ai tuoi coetanei per affrontare al meglio le prossime competizioni Cyber?

In primo luogo è necessario avere un corpo docente che possa prepararti ad affrontare questo tipo di sfide. Conoscere ciò che si andrà ad affrontare è sicuramente fondamentale quanto il background e la preparazione. Un consiglio che posso dare ai giovani che parteciperanno a queste competizioni è applicarsi come se non ci fosse un domani e allargare i propri orizzonti.

Credi che queste competizioni possano dare un valore aggiunto agli studenti che stanno terminando gli studi per una futura posizione lavorativa? Personalmente hai una tua vocazione specialistica in questo universo Cyber?

Il CyberChallenge.it rappresenta una base pratica molto importante quindi chiunque partecipi a questa competizione Challenge si trova un passo avanti agli altri. Personalmente qualche azienda mi ha già chiamato. Per ora sto ancora completando il mio percorso di laurea ma al termine sicuramente ne accetterò una. Ho infatti intenzione di seguire un'azienda che si occupa di Penetration Testing e Malware Analysis, che tra l'altro riguarda il Reversing che era una delle categorie di CTF.

Svelaci un'ultima curiosità. Da dove nasce la tua passione per la Cybersecuity?

Prima di tutto è nata una passione per l'informatica. È stato più che altro un caso. Teoricamente non avrei dovuto neanche prendere l'indirizzo informatico, avrei voluto studiare Medicina. Solo all'ultimo ho scelto di cambiare strada proprio per poter coltivare in pieno la mia passione nascosta e in particolare l'argomento che mi piaceva di più in informatica era la Sicurezza durante la navigazione sul web dei giochi, le CTF. Questi giochi sono presi molto sul serio nel settore della Cybersecurity perché rappresentano simulazioni di vulnerabilità che potrebbero interessare un qualsiasi servizio online. Per questo motivo, proprio allora mi sono chiesto: se queste CTF per me sono dei giochi e questi giochi per molti rappresentano un vero e proprio lavoro, perché non trasformare questa passione in lavoro? ■

Intervista VIP con il Brig. Gen. Anton ROG, Capo del National Cyberint Centre, Romania

Anton Rog

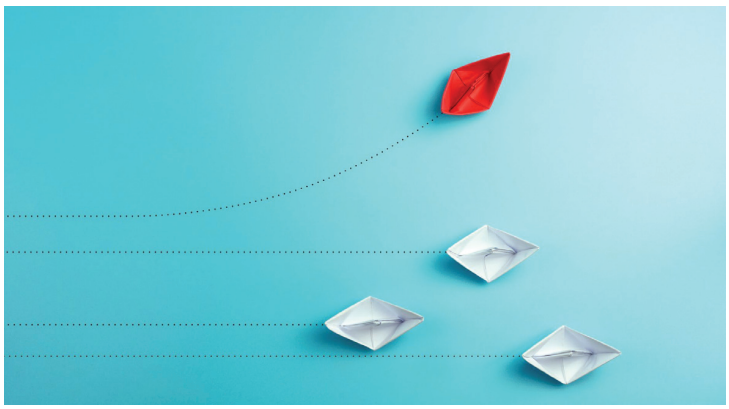
Autore: Laurent Chrzanovski

BIO

Il Generale di brigata Anton Rog è Capo del National CYBERINT Centre del Servizio di intelligence rumeno (SRI). Il CYBERINT è il centro responsabile dell'individuazione, analisi e contrasto proattivo alle minacce informatiche 24/7 contro sistemi e reti critiche per la sicurezza nazionale della Romania. Anton Rog ha ricoperto diverse posizioni di sviluppo tecnico tra cui progettazione di software e sistemi. Ha anche lavorato come vicedirettore all'interno del Dipartimento Centrale IT&C dello SRI. È attivo con la comunità accademica come professore associato presso DRESMARA (Dipartimento Regionale Di Studi Per La Gestione Delle Risorse Della Difesa) di Brasov. Anton Rog si è laureato presso l'Università di Bucarest nel 1998 con un B.S. in informatica e ha conseguito nel 2011 presso DRESMARA un diploma post-laurea in "Program and Project Management". Ha ricevuto il premio Knight of the Order Manhood and Faith nel 2014 e Knight of the Order of Military Virtue nel 2005 da due differenti Presidenti della Romania.

A proposito della tua persona. Dopo anni di dedizione alla progettazione, allo sviluppo e alla garanzia della buona funzionalità dei sistemi IT&C - hai raggiunto la posizione di vice capo del dipartimento IT&C centrale dello SRI - sei passato* "dall'altra parte della linea"*, vale a dire a difendere e proteggere Sistemi IT&C. Cosa ti ha spinto a prendere la decisione di fare questo* "passaggio"*, piuttosto raro tra gli specialisti IT?

Ho lavorato nel servizio di intelligence rumeno (SRI) per oltre 20 anni e fino all'inizio del 2017 ero impegnato in un'area che aveva molteplici compiti



tecnici. Non ho scelto di *"cambiare fronte"* a favore del settore digitale, ma la direzione dello SRI ha ritenuto che, a quel tempo, rappresentassi una buona risorsa da impiegare per la direzione del Centro nazionale CYBERINT, posizione vacante dopo il pensionamento del mio predecessore. Anche se inizialmente ho ritenuto che il mio profilo, basato sullo sviluppo e sulla creatività, non fosse compatibile con il lavoro specifico da realizzare nella cybersecurity, in realtà poi sono riuscito rapidamente ad inserirmi e integrarmi all'interno del team e, quindi, posso dire che mi è piaciuto essere il "jolly" dello SRI, posizione che ho cercato di valorizzare dando il massimo.

Pay-per-service. Contrariamente alla maggior parte degli stati dell'UE, i tuoi Servizi difendono l'intero paese come un dovere e senza alcun compenso per il lavoro svolto. Per essere più precisi, anche se lo Stato centrale rumeno controlla pochi servizi elettronici, città metropolitane come Sibiu offrono privatamente ai cittadini un accesso totale a molti documenti sensibili (fiscalità, catasto, situazione familiare, ecc.) proponendo soluzioni online per il pagamento di tasse, servizi, multe, etc. Anche In Francia, vi è una situazione analoga dove è possibile scegliere tra l'ANSSI (Agenzia Nazionale per la Sicurezza dei Sistemi di Informazione) e società private per la cybersecurity. In Romania, troviamo da tempo una condizione similare per il trasporto di importanti manufatti all'interno dei musei: è possibile pagare la scorta del trasporto alla Gendarmerie (= Carabinieri, n.d.r.) o scegliere una delle compagnie di sicurezza private riconosciute dallo Stato. Cosa ne pensi di questa situazione e della sua applicabilità in Romania, con i suoi vantaggi e svantaggi?

In Romania non tutti i servizi demografici godono di una buona implementazione online – certificati di nascita, matrimonio, ecc. - questa implementazione è un processo che tutt'oggi è in corso. Il pagamento delle tasse viene effettuato online già in diverse città della Romania, non solo a Sibiu, compresa ovviamente la capitale, Bucarest.

Per quanto riguarda il confronto con il modello francese, ritengo che ogni Stato membro dell'UE definisca la propria legislazione. In Romania esiste un unico Centro per il pagamento delle tasse, www.ghiseul.ro. Il sito è gestito dal *Romanian Agency for Digital Agenda* e supportato dall'*Electronic Payments Association of Romania*. L'aspetto più importante in questo caso è che eventuali tasse e commissioni non sono addebitate ai contribuenti che optano per il pagamento attraverso il sito www.ghiseul.ro. Di conseguenza, questo nuovo servizio che conta circa mezzo milione di utenti attivi consente il pagamento delle tasse senza commissioni in tempo reale.

GHIȘEUL.RO

Attribuzione di responsabilità reali vs. attribuzioni di responsabilità politiche: negli ultimi congressi, hai mostrato solide e comprovate attribuzioni di responsabilità di attacchi, al contrario di tutte le attribuzioni politiche "mainstream" che principalmente possiamo leggere sui media di tutto il mondo. Pensi che si arriverà mai a una maturità dei media europei nel diffondere esclusivamente esempi come i tuoi o questi ultimi continueranno a essere trascurati sotto tonnellate di "attribuzioni di responsabilità immediate" che forniscono eccellenti "notizie dell'ultim'ora"? Cosa si potrebbe fare per incoraggiare la mediatizzazione di casi reali che hanno visto mesi di lavoro alle loro spalle?

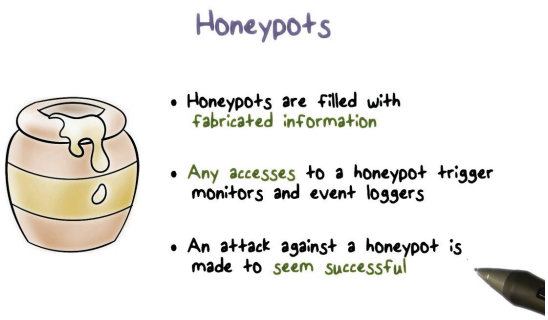
Entrambi i tipi di attribuzione di responsabilità sono ugualmente importanti: sia tecnico che politico, il secondo è costruito sul primo. Il National CYBERINT Center è l'attore principale nella definizione dell'attribuzione tecnica di responsabilità relative agli attacchi informatici supportati da attori governativi. Nel nostro paese, è stato creato un meccanismo speciale, sotto la firma del Presidente della Romania, che ci consente di prendere parte a iniziative internazionali di tipo *"blame and shame"*, che hanno un impatto considerevole sui media. Ad esempio, nel 2018, ho preso parte a un'azione internazionale circa l'ondata

di attacchi della campagna APT28 congiuntamente agli Stati promotori: il Regno Unito e gli Stati Uniti seguiti da altri Stati membri dell'Unione Europea. A mio avviso, è importante garantire una copertura mediatica delle responsabilità politiche basate sull'esperienza tecnica perché solo in questo caso è prevedibile un suo massiccio impatto. Una volta che questi attacchi informatici sono stati scoperti e vengono attribuiti all'autore dalla maggior parte delle vittime dello Stato colpito, lo sforzo congiunto e associato si tradurrà in una sostanziale copertura mediatica internazionale.

Fino a cinque anni fa, la maggior parte delle Agenzie statali dell'UE come la tua parlava regolarmente dell'utilizzo proficuo degli «honeypot». Questo termine è oramai piombato nell'oblio. Questo perché è una

tecnica diffusa per cercare di distrarre almeno ad minimam l'attenzione dei «cattivi» o, al contrario, perché le tecnologie consentono agli aggressori di riconoscerli troppo facilmente?

Nell'evoluzione dei fenomeni di cybersecurity, gli "honeypot" hanno giocato e svolgono il loro ruolo, ma non possono essere considerati soluzioni adatte a ogni tipo di attacco informatico. Quando si parla di attacchi governativi, il malware utilizzato è estremamente



complesso e in molti casi in grado di rilevare facilmente tali "honeypot". L'area in cui questa soluzione informatica genera successi è il classico crimine informatico volto a ottenere benefici finanziari con mezzi di frode informatica.

Ritorsione e proattività: l'anno scorso i cittadini svizzeri hanno votato in modo compatto a favore delle polizze cantonali e del vostro omologo, FedPol, al fine di creare, sotto il controllo di un procuratore, falsi profili commerciali su social media e qualsiasi altro strumento utile per esaminare e intervenire nell'immediato in frodi, spionaggio economico o operazioni di sabotaggio. Da anni, i tuoi colleghi in Olanda e in India hanno il "diritto legale" di rispondere in caso di attacchi. I Servizi lo fanno sistematicamente, attraverso le loro agenzie o tramite i "privateers". Cosa ne pensi di questa situazione? Ottenere tale diritto sarebbe un vantaggio per una Romania più cyber-sicura o aumenterebbe semplicemente la quantità di uomini e risorse necessarie per svolgere quei compiti senza un risultato legittimato?

Ritengo che tali strumenti possano supportare in modo proattivo e molto efficace la prevenzione delle minacce nel cyberspazio e possano essere d'aiuto nell'indagine su alcuni incidenti che si sono già verificati. Sfortunatamente, in Romania, non abbiamo una legge che regola la sicurezza e la difesa informatica che al contrario potrebbe rappresentare uno strumento decisamente utile. Tuttavia, il diritto internazionale, applicato anche in Romania, consente l'uso di misure di ritorsione progressiva in caso di attacchi informatici. In questo quadro, la dimostrazione del legame tra un attore cibernetico e un attore statale riveste un'importanza speciale perché solo il raggiungimento di queste condizioni può consentire l'applicazione delle disposizioni del diritto internazionale.

In una prospettiva di collaborazione pubblico-privato, quali sono i tuoi progetti e desideri per gli anni a venire, per una Romania più sicura. Cosa è stato recentemente realizzato e cosa resta da fare?

Tra le principali iniziative future che il National CYBERINT Center intende realizzare come partenariato pubblico-privato, vorrei menzionare il rafforzamento dei programmi universitari nelle 21 università che hanno concordato di avviare programmi di studio approfonditi post-laurea in cybersecurity (di breve durata o anche master) e la prosecuzione del nostro progetto pilota dedicato all'introduzione di concetti di cybersecurity e igiene informatica nei programmi di scuole superiori nazionali dei college con specializzazioni IT. Un secondo obiettivo è quello di aumentare la qualità delle esercitazioni nazionali fornendo un numero costante di player e analisti come ad esempio l'esercitazione nazionale in cybersecurity, CyDEx, ma anche quello di intensificare il numero le conferenze nazionali sulla cybersecurity, come ad esempio la conferenza internazionale *"Strategic Partnership Romania-US cyber security"* e il congresso organizzato nella città di Sibiu *"Cybersecurity dialogues - Romania"*.

A livello legislativo, è estremamente importante intensificare l'attuazione delle disposizioni della direttiva NIS, che aumenterà la sicurezza dei servizi IT e degli operatori dei servizi essenziali; è inoltre essenziale creare in Romania un mercato solido per la cybersecurity. Ultimo ma non meno importante, a livello istituzionale, penso che dovremmo creare un hub per lo scambio di informazioni tra i principali attori responsabili nella cybersecurity all'interno delle diverse istituzioni pubbliche rumene coinvolte, che può essere costruito seguendo e adottando i modelli stabiliti già da altri paesi, come USA, Regno Unito o Israele. ■

TIBER-EU il framework europeo per testare la resilienza del settore finanziario agli attacchi informatici

Autore: Giancarlo Butti

Il Consiglio direttivo della BCE ha approvato nella primavera del 2017 la strategia di supervisione per la resilienza cibernetica delle infrastrutture di mercato europee con il fine di assicurare un'applicazione comune e coerente con la ***Guidance on cyber resilience for financial market infrastructures***[1] *nell'ambito dell'Eurosistema. Fra le iniziative vi è anche la predisposizione di un quadro di riferimento per l'esecuzione di test avanzati sui sistemi informativi. Vediamone in breve le principali caratteristiche.*

Con la denominazione di TIBER[2]-EU viene identificato un framework comune transnazionale per l'esecuzione di test che prevede l'uso di una varietà di tecniche per simulare un attacco alle funzioni critiche di un'entità e ai sistemi sottostanti (cioè persone, processi e tecnologie) al fine di valutarne la resilienza.

Gli obiettivi sono aiutare le entità a ottenere informazioni sulle loro capacità di protezione, rilevamento e risposta e per aiutarle a combattere gli attacchi informatici.

Il framework facilita inoltre i test per le entità transfrontaliere sotto la supervisione di diverse autorità, facilitando un approccio europeo armonizzato nei confronti dei test basati sull'intelligence che imitano le tattiche, le tecniche e le procedure dei veri hacker.

Tale attività, come è noto soprattutto a chi ha partecipato anche ad altre tipologie di test (come ad esempio quelle sulla business continuity) sono rischiose (e costose) e vanno accuratamente preparate.

Questo fa sì che i rischi che derivano da tali azioni, quali l'individuazione di informazioni sulle vulnerabilità dell'entità sottoposta a test ed altre informazioni riservate da parte dei soggetti che partecipano alle attività di verifica, nonché possibili malfunzionamenti o anche la perdita o diffusione di dati, devono essere preventivamente individuati e gestiti.

È inoltre particolarmente importante che tali test siano effettuati da soggetti particolarmente qualificati e che offrano adeguate garanzie; il framework quindi fornisce anche indicazioni su come effettuare una valutazione dei possibili fornitori.[3]

Gli obiettivi di TIBER-EU comprendono fra gli altri:

- migliorare la cyber resilienza delle entità e del settore finanziario in generale;
- standardizzare e armonizzare il modo in cui le entità eseguono i test in tutta l'UE, garantendo al contempo a ciascuna giurisdizione un certo grado di flessibilità per adattare il quadro in base alle sue specificità;
- fornire indicazioni alle autorità su come stabilire, attuare e gestire questa forma di test a livello nazionale o europeo;

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.

- valutare anche gli aspetti giurisdizionali per i test di entità multinazionali;
- favorire la cooperazione internazionale fra i vari soggetti coinvolti;
- etc.

Lo svolgimento dei test secondo il processo TIBER-UE prevede tre fasi:

- una fase di preparazione
- la fase di test
- una fase di chiusura

Come meglio dettagliato nelle tabelle qui sotto riportate:

Table 2
Preparation phase

Requirements	Mandatory	Optional
For each test, there is a White Team (WT), independent TCT (and Test Manager), and external TI/RT providers.	✓	
The national intelligence agency/national cyber security centre/high-tech crime unit is involved in each test.		✓
Once the procurement process has been completed, there are appropriate contracts in place between the different stakeholders, with relevant controls embedded into the contracts, to facilitate a controlled test (in a discreet manner).	✓	
Prior to conducting the test, the WT conducts a risk assessment and then puts in place all the necessary risk management controls, processes and procedures to facilitate a controlled test.	✓	
Throughout the end-to-end test process, in all documentation and communication between stakeholders a code name is used to conceal the identity of the entity being tested.	✓	
At the outset of the test process, there is a launch meeting which includes the WT and TCT.	✓	
The launch meeting also includes other relevant authorities and the TI/RT providers.		✓
The scope of the test includes critical functions (CFs), as well as the people, processes, and technology and databases that support the delivery of CFs. This is documented in the TIBER-EU Scope Specification document and signed off in the attestation by the board.	✓	
The entity expands the scope of the test beyond the CFs and includes other functions and processes.		✓
During the scoping phase, the WT (with agreement from the TCT), sets "flags", which are targets or objectives, that the RT provider aims to meet during the test.	✓	
The test is conducted on live production systems.	✓	
Only the WT and TCT are informed about the test, its details and the timings – all other staff members (i.e. Blue Team, BT) remain unaware of the test.	✓	
Only TI/RT providers that meet the minimum requirements set out in the TIBER-EU Services Procurement Guidelines can undertake the TIBER-EU test. The TI/RT providers will be TIBER-EU-certified and accredited once the EU has these capabilities in place.	✓	

Table 3
Threat intelligence and red team testing phase

Requirements	Mandatory	Optional
For each test, an external TI provider produces a dedicated Targeted Threat Intelligence Report (TTI Report) on the entity being tested. Where infrastructure has been outsourced and a third party is included in the scope of the test, the TTI Report also includes information about that third party.	✓	
For each national implementation, a Generic Threat Landscape Report (GTL Report) for the country's financial sector is produced and maintained, and is used to help inform the TTI Report.		✓
For each threat intelligence report (TTI and GTL), the national intelligence agency/national cyber security centre/high-tech crime unit is involved to provide feedback.		✓
For each TTI Report on the entity, the TI provider sets out multiple threat scenarios which can be used by the RT provider.	✓	
The TI provider holds a handover session with the RT provider, providing the basis for the threat scenarios.	✓	
Following the handover, the TI provider continues to be engaged during the testing phase and provides additional up-to-date, credible threat intelligence to the RT provider, where needed.		✓
The RT provider develops multiple attack scenarios, based on the TTI Report. This is documented in the Red Team Test Plan and shared with the WT and TCT.	✓	
The jurisdiction, in its implementation of the TIBER framework, allows physical red teaming in the scope of the methodology for the TIBER test (e.g. planting a device at the entity), provided all necessary precautions are taken.		✓
The RT provider executes the attack based on the scenarios (with some flexibility) in the Red Team Test Plan and goes through each of the phases of the kill chain methodology. Where needed, a "leg-up" will be provided by the entity.	✓	
During the test, the RT provider keeps the WT and TCT informed about progress, "capture the flag" moments, the possible need for leg-ups, etc. The RT provider takes a stage-by-stage approach and consults the WT and TCT at all critical points to ensure a controlled test.	✓	
The duration of the red team test is proportionate to the scope, size of the entity, complexity of threat scenarios, etc. Sufficient time is allocated to testing to guarantee that a comprehensive test has been conducted across the enterprise. Experience suggests that a period of at least 10–12 weeks is required.	✓	

I test TIBER-UE devono essere eseguiti senza la conoscenza della sicurezza dell'entità target o della capacità di risposta (ovvero Blue Team, BT). Solo un piccolo gruppo dell'entità, indicato come White Team (WT), conosce il test. Questo per garantire che il test sia in grado di valutare l'efficacia dell'entità target in grado di proteggere i suoi sistemi critici e l'efficacia con cui è in grado di rilevare e rispondere agli attacchi.

Table 4
Closure phase

Requirements	Mandatory	Optional
At the end of the test, the RT provider produces a Red Team Test Report, outlining the findings from the test.	✓	
The entity's BT is informed of the test and uses the Red Team Test Report to deliver its own Blue Team Report. In the Blue Team Report, the BT maps its actions alongside the RT provider's Team actions.	✓	
At the end of the test, the RT provider, the BT and the WT conduct an interactive replay of the test, where possible using live production systems, to review the impact of the actions of the RT provider.	✓	
The TCT, supervisors/overseers and TI provider are also present during these replay workshops.		✓
A purple teaming element is added in which the BT and the RT provider can work together to see which other steps could have been taken by the RT provider and how the BT could have responded to those steps.		✓
At the end of the test, there is a 360-degree feedback meeting which includes the entity, TI/RT providers and TCT. In this meeting, the parties review the TIBER-EU test process and give feedback.	✓	
After the BT and RT provider replay and 360-degree feedback workshop, the entity produces a Remediation Plan to address the findings. The Remediation Plan is agreed with the supervisor and/or overseer as part of their planning and control cycle.	✓	
The entity produces a Test Summary Report, which it shares with the lead authority.	✓	
The entity's board and the TI/RT providers sign an attestation to validate the true and fair conduct of the TIBER-EU test (to enable recognition by other relevant authorities).	✓	
If mutually agreed, the lead authority and/or the entity share the Test Summary Report and attestation with other relevant authorities (where applicable).	✓	
The TCT in each jurisdiction analyses the results of all the TIBER tests and the lessons learned from the 360-degree feedback meetings to produce high-level, aggregated findings. This information is used to enhance sector resilience and improve the TIBER-XX framework.	✓	

L'intelligence-led red team testing (o red teaming)[4]

Per misurare la qualità delle difese di un'impresa target viene in primo luogo chiesto a un gruppo di investigatori (threat intelligence providers) di valutare le modalità attraverso le quali soggetti ostili potrebbero sfruttare le vulnerabilità organizzative, procedurali e tecnologiche dell'organizzazione, e di descrivere tali vulnerabilità in un targeted threat intelligence report. Sulla base di tale rapporto, un secondo gruppo indipendente di "pseudo-attaccanti" (denominato red team, secondo un'espressione mutuata dalle esercitazioni militari) pianifica ed esegue appositi esercizi di simulazione allo scopo di valutare le difese dell'obiettivo dell'aggressione.

Le pubblicazioni del framework

La descrizione della metodologia è raccolta in 3 diverse pubblicazioni:

TIBER-EU FRAMEWORK - How to implement the European framework for Threat Intelligence-based Ethical Red Teaming

Che descrive nel dettaglio le modalità per l'esecuzione dei test, come sopra evidenziato

TIBER-EU Framework - Services Procurement Guidelines

Che fornisce, ad esempio, i requisiti dei Threat Intelligence Provider, dei Red Team Provider e gli strumenti per la loro valutazioni, quali ad esempio questionari e check list, come quella qui sotto parzialmente riprodotta:

Example of TI provider agreement checklist

Clause

Intellectual property

- The contract includes agreements on intellectual property (IP), stating that IP remains with the entitled party.

Non-disclosure agreement

- The contract has a non-disclosure agreement, stating as a minimum that:
- information will not be used outside of the context of TIBER-EU
- information will only be used for the purpose for which it was provided/collected; and
- the TI provider must ensure that all staff involved in the service (including staff provided by external parties) adhere to the agreements made concerning security and confidentiality.

Sharing threat intelligence information

- The threat intelligence report that the entity receives is the property of the entity. The entity therefore has the right to share this information with other relevant parties. The TI provider cannot share this information with any other party without the prior approval of the entity.

Information security

- The TI provider demonstrates its security measures and procedures and how these operate. For example:
- the TI provider has a security policy, approved by its Board of Directors;
- the TI provider has a demonstrable effective Information Security Management System;
- information security is an integral part of the TI provider's risk management processes;
- every risk-mitigating measure, including those regarding information security, is documented and reviewed regularly;
- information systems used for storing and processing information regarding the entity are adequately protected and secured using state of the art methods, including periodical penetration tests and vulnerability assessments;
- information asset management is in place including inventories, retention and secure deletion and destruction;
- all information related to TIBER-EU is accessed on a need to know basis. This is controlled by a combination of pro-cedural and technical measures, and all access to this information is logged and monitored.

Viene anche fornita una tabella con un elenco delle possibili certificazioni che qualificano il personale addetto alle operazioni e le stesse strutture che si offrono quali TI o RT provider.

TIBER-EU White Team Guidance - The roles and responsibilities of the White Team in a Threat Intelligence-based Ethical Red Teaming test, che indica i ruoli e le responsabilità del White Team.

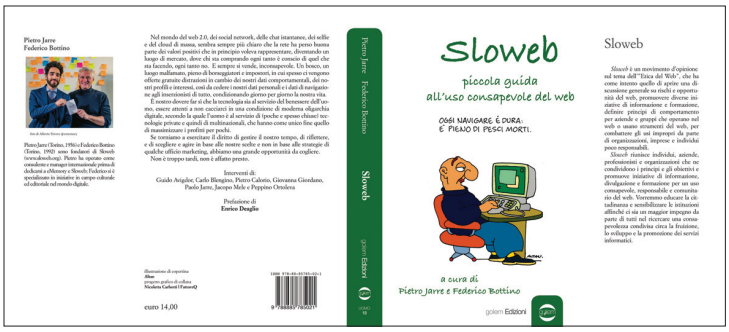
Come per tutte le altre normative e pubblicazioni nell'ambito della sicurezza emanate dalle istituzioni nazionali od europee, anche in questo caso è possibile anche da parte di aziende di altri settori utilizzare questi documenti, liberamente accessibili sul sito della Banca Centrale Europea[5], quali buone pratiche di riferimento. ■

1 Pubblicata nel 2016 dal CPMI-Iosco, la guidance indica metodi e strumenti per garantire la continuità operativa delle infrastrutture di mercato in caso di attacchi cibernetici
2 TIBER, ovveroThreat Intelligence-based Ethical Red Teaming
3 TIBER-EU Framework Services Procurement Guidelines
4 Tratto da: Sicurezza cibernetica:il contributo della Banca d'Italia e dell'Ivass
5 https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf

Memoria e identità sono valori forti che dobbiamo coltivare nella società digitale: ci dicono chi siamo e da dove veniamo

Autore: Massimiliano Cannata

Pietro Jarre



Sloweb *è un termine che evoca lentezza. Sloweb nasce per indurre a un ritorno della riflessione in tempi più votati alla superficialità e alla reazione istintiva?*

La sua lettura è corretta. Lentezza come diritto a pensarci bene. Con Sloweb, dice Mario Perini, psicoanalista, *l'uomo di oggi deve riappropriarsi del diritto a una mente lenta e riflessiva che usa una tecnologia veloce*. Stiamo perdendo la capacità di riflettere, come pesci un poco stolti siamo distratti dai mille oggetti lucenti che ci turbinano intorno. La stessa attenzione – che precede la riflessione – è compromessa, ridotta a pochi minuti nel migliore dei casi. Io stesso mi rendo conto che faccio fatica a leggere 10 – 20 pagine di un libro senza mai interrompermi, dare un'occhiata allo smartphone, fare qualcosa d'altro. Più in particolare va precisato che il nome della nostra Associazione è derivato da Slowfood, ma anche da Slowmedicine, che perora la causa di una medicina sobria rispettosa e giusta. Al momento di decidere che logo adottare per "Sloweb" noi abbiamo pensato di non ricorrere ad animali e simboli simili, e piuttosto scrivere semplicemente "Sloweb" in corsivo come fosse scritto con penna ed inchiostro da un alunno di prima, che scrive lentamente e con attenzione pensa, e mentre pensa cresce… tiene la lingua fuori per lo sforzo, si concentra, e cresce.

Molto bella questa immagine che evoca la tensione della crescita verso una direzione che non sempre conosciamo. L'attività della vostra Associazione si fonda su due valori - chiave: etica e responsabilità. Come si declinano nell'era del web questi concetti che hanno una lunga tradizione filosofica alle spalle?

Per qualche tempo ho usato le parole "uso responsabile" e "uso consapevole" del web senza riflettere che si tratta di due fronti diversi di una comune radice, l'etica: *le aziende* devono essere indotte ad un uso responsabile del web, che significa un uso etico, per esempio a non produrre

BIO

Pietro Jarre – 63 anni ingegnere fondatore di Sloweb e ideatore di eMemory e eLegacy. Promuove servizi web di informEtica, eventi di educazione digitale, pubblicazioni e iniziative culturali sull'uso responsabile e consapevole del web. Nell'intervista che fa riferimento al libro *"Sloweb - Piccola Guida all'uso responsabile del web"* da lui curato con *Federico Bottino, (Golem Edizioni)*, Jarre con grande efficacia fa vedere le grandi potenzialità, ma anche i rischi connessi all'uso del web. Conoscenza della storia, rispetto della diversità, consapevolezza sono termini chiave che l'uomo di oggi deve curare e praticare, per non trasformarsi da "Sapiens Sapiens" a Stupidus Stupidus, per usare un'immagine dello psicanalista Vittorino Andreoli.

software che dia dipendenza, e non rubare informazioni ai propri utenti. Chi le deve indurre in questa direzione? I cittadini e le istituzioni dello Stato. *Gli utenti,* dal canto loro, devono avere / essere indotti e guidati ad un uso consapevole ed etico. Come per l'educazione sessuale, devono conoscere rischi e opportunità, pericoli e piaceri nell'uso del web. Oggi si parla molto di etica del web intorno al tema *privacy,* ma penso non sia più rimandabile la discussione e le azioni circa il tema *disuguaglianza*. E' etico produrre, offrire, diffondere, un prodotto che serve all'accumulazione illimitata del denaro di molti nelle mani di pochi? Il web ha una straordinaria capacità di penetrazione in ogni gruppo sociale, offrendo opportunità e alcuni rischi non piccoli, eppure *si smercia dappertutto* e con poche istruzioni per l'uso, non come le sigarette che invece sono vendute a caro prezzo agli adulti solo maggiorenni e solo in negozi con la T e non a caso lo stemma dello Stato.

Navigare un esercizio non facile e pieno di rischi

Navigare è dura troppi pesci morti recita il distico che campeggia nella copertina del volume. Possiamo spiegare meglio questa efficace metafora?

Nel 2017 con Federico Bottino abbiamo chiesto a Francesco Tullio Altan una vignetta che potesse illustrare il libro e lui con incredibile gentilezza ci ha regalato quella dell'omino che pronuncia appunto questa frase. In rete si naviga, ed è sempre più difficile trovare roba buona, è pieno di porcheriole, di distrazioni e pesci morti, appunto. Secondo me i suoi "pesci morti" rappresentano le fake news, il pattume in generale. Pensi alla piramide della conoscenza, che al vertice ha la saggezza, alla base il puro "dato". Beh, non v'è chi non veda che la rete è sempre più piena di "dati", quasi sempre non validati e non duraturi, quasi sempre di scarso valore, e in tutto ciò c'è un disequilibrio crescente, tanto pettegolezzo, poca riflessione, nessuna saggezza: come un iceberg la cui base spinge verso l'alto, la piramide un giorno si cappotterà, e il vertice della conoscenza sarà schiacciato dai big data, con gran puzza di marciume dovunque, e appunto tanti pesci morti.

Le parole sono importanti anche per chi fa innovazione. "Il linguaggio è il nostro mondo" si potrebbe dire parafrasando una celebre affermazione di Wittgenstein. Il glossario che pubblicate all'interno del volume evoca questa finalità?

Certamente. Le parole hanno significati diversi per i diversi soggetti parlanti, questo fa capire quanto sia difficile costruire qualcosa di buono insieme, figuriamoci se parliamo di innovazione. Mi permetta un semplice esempio: internet è una rete fisica fatta di cavi, piloni, schede in plastica e pezzi fatti con quasi tutti gli elementi presenti sulla Tavola Periodica di Mendeleev. Il web NO. *Internet NON è etereo, il web si*, dice Giovanna Giordano, fondatrice di Sloweb. Internet consuma materiali, energia elettrica, il suo uso implica produzione di anidride carbonica (e notiamolo: in misura crescente del 15 – 20% annuo, già oggi l'ICT produce CO2 in misura maggiore di tutta l'industria avionica…) Non possiamo dire "internet" intendendo "il web" e viceversa. Si le parole sono importanti.

Il valore della memoria

Specificazione linguistica essenziale, grazie per avercelo ricordato, perché in effetti i due termini vengono quasi sempre usati come sinonimi.

Vorrei ora toccare un altro tema con Lei, quello della Memoria e della eredità digitale, mission importanti per Sloweb, aggiungerei decisive in una società schiacciata sul presente. Che tipo di lavoro state portando avanti su questo delicato terreno?

In Sloweb alcuni di noi si dedicano all'educazione (non solo l'alfabetizzazione) digitale, altri a metodi per includere categorie svantaggiate nell'uso – consapevole – del web. Con Alessandro Macagno e altri io mi dedico per esperienza professionale e storia personale ai temi della memoria e dell'eredità digitale. Su questi campi facciamo tesoro delle esperienze e delle idee di specialisti in psicologia, insegnanti, storici e archivisti, e soprattutto degli utenti di eMemory e di eLegacy e dei responsabili HR, ICT, marketing e strategia delle aziende con cui interagiamo ogni giorno. eMemory e eLegacy sono le piattaforme che abbiamo creato per aiutare famiglie,

comunità e aziende a selezionare memorie ricordi e documenti che contano, a valorizzare, a proteggerli in ambienti non profilati, a definirne il destino per poterli tramandare in sicurezza. L'homo sapiens è qui perché ha potuto fermarsi nella caccia e nella raccolta, e attorno a un fuoco raccontarsi di rischi e opportunità, insegnando ai giovani della tribù cosa il futuro può portare, e come affrontarlo. Non dico nulla che non si sappia, ma oggi in troppi non ci rendiamo conto e non combattiamo il fatto che un uso improprio delle tecnologie digitali porta alla perdita di tempo, di riflessione, delle storie, e quindi e presto della identità e della memoria.

Quali sono i pericoli connessi a questa deriva?

Tendiamo a delegare ogni cosa da ricordare al nostro smartphone, e l'età cui inizia la demenza senile si abbassa… e tra perdita di memoria e storia è forse così che l'umanità sparirà, senza sapere chi siamo, senza saper affrontare i rischi di sempre, perché nessuno la sera ci racconterà più del lupo e dei tre porcellini e di quando la nonna faceva il pane per la settimana successiva e per tutto il paese. E nessuno seleziona ciò che è importante; di mia nonna ho 10 foto, e queste bastano per raccontare la sua straordinaria storia di coraggio attraverso il '900; di mia madre ne ho 100. Io rischio, se non seleziono e valorizzo, di lasciare 100000 fotografie a mio nipote – e lui cosa farà? Le butterà, perché non gli avrò lasciato – in realtà - proprio nulla. L'eredità digitale è un tema che sta emergendo con prepotenza tra noi: lasciamo ciò che non vogliamo e non lasciamo ciò che importa (incluse le password per i bitcoin, alle volte!). Un grande caos, che richiede una guida giuridica – che con il GDPR inizia ad esserci – e strumenti informatici – che noi prima di altri stiamo predisponendo.

La memoria è un grande patrimonio, mortificato da un processo di rimozione e da una dilagante ignoranza della storia che non può lasciarci indifferenti. Qual è la sua valutazione in merito?

Sulla memoria, e l'importanza di salvare ciò che conta per crescere bene, le racconto una piccola storia. Due anni fa con Alberto Trivero abbiamo fatto fare 500 scatole da scarpe con il marchio di eMemory, in un bel colore arancione, come omaggio per i primi utenti. Ne sono avanzate alcune, e quando incontro un nonno o una mamma gliene regalo una o due, spiegando che sono *le scatole della memoria* e si usano così: insegniamo ai bambini a tenere conto, apprezzare e valorizzare, piccoli elementi – una fotografia, il ciuccio o il pupazzo, il primo disegno, quella foto particolare – della loro vita. Prima noi adulti, , poi insieme a loro, poi solo loro apriranno di tanto in tanto la scatola, per salvarci un biglietto, un sasso, una cartolina (!). Loro sapranno meglio chi sono, avranno le tracce di sé e avranno imparato a tenerle, e quando a 20 anni magari andranno fuori casa, noi ci metteremo

ancora il libretto dei vaccini, e loro potranno portare con sé quello che serve a ricordare chi sono, da dove vengono, e quanto lontano possono andare. A 20 anni avranno già cambiato invece 5 o 10 smartphone, e perso i volti e i cuoricini dei primi amori, e gli infiniti byte di immagini tutte alla rinfusa, ma nella scatola della memoria avranno quello che serve per andare lontano.

Avete creato quella che i greci definivano una koinè di studiosi, intellettuali e domani giovani per riflettere su un grande fenomeno come quello della Rete. Aveva ragione Stefano Rodotà a sostenere la definizione di una costituzione per internet, che rappresenta il più grande spazio pubblico di cui l'umanità abbia mai disposto dall'origine della storia a oggi?

Se tre anni fa pensavo da ingegnere che tutto questo avesse molto a che fare con la tecnologia, sempre di più sto capendo che invece *ha a che fare con i diritti, la politica, la filosofia, l'etica appunto;* e non dimentichiamo che gli informatici oggi sono i tecnici che più a fondo entrano nella nostra anima, e proprio loro, gli informatici, non hanno studiato né teologia, né psicologia, e neppure i rudimenti dell'etica di base come i medici o gli ingegneri. Non hanno un albo professionale, non rispondo che a sè stessi. Così accade che troppi tra loro pensano che *ciò che è tecnicamente fattibile sia automaticamente lecito!* E i risultati li vediamo. Quanto a Stefano Rodotà e ai diritti posso dire che provengo da anni di esperienza globale finalizzata a far evolvere il tema della responsabilità sociale dell'impresa da patrimonio di poche multinazionali a norma e linea guida adottate a livello delle Nazioni Unite e non posso che essere d'accordo.

Occorre una dichiarazione dei diritti dell'uomo digitale

Rodotà oltre ad essere un grande giurista ha lavorato molto sulla realtà di Internet e su quella che definiva la "tutela del corpo elettronico". Sicuramente ci ha visto giusto alla luce dell'evoluzione di questi ultimi anni, non crede?

Si, certo, e aggiungerei pensando al web che in questo campo avremmo un *urgente bisogno* di una *Dichiarazione Universale dei Diritti Digitali dell'uomo* (che includa l'impatto ambientale, sociale ed economico del digitale). E aggiungo ancora che l'Europa ha una responsabilità e un'opportunità specifica in merito, grazie al GDPR che – sia detto per inciso – in Nord America molti ci invidiano. A proposito: per sviluppare il software

di eLegacy abbiamo lavorato a stretto contatto proprio con legali e giuristi – Pietro Calorio e Alessandro D'Arminio Monforte - e sfruttato appieno il GDPR, che offre possibilità molto vaste. Con eLegacy riconosci la tua presenza digitale come il tuo volto in uno specchio, e grazie al GDPR puoi disiscriverti, cancellare e ordinare i tuoi account, dire cosa DEVE succedere nel caso in cui tu ti ammalassi o morissi: ciò che lasci, ciò che NON lasci, i tuoi diritti ora e per sempre.

Chiuderei con una domanda più generale. Sicurezza e libertà sono i concetti antinomici che segnano da sempre il cammino dell'uomo e in particolare connotano il delicato rapporto tra l'individuo e gli strumenti della tecnologia. È possibile arrivare a un equilibrio virtuoso in questa essenziale polarità?

Più che generale, mi scusi, ma questa è una domanda per altri, per i filosofi della Scienza… Forse Lei si vuole riferire allo sviluppo tecnologico in ambito bellico e ai suoi benefici in termini di sicurezza e libertà? Negli ultimi decenni il mondo è stato più "sicuro e libero" per molti (non per tutti) forse anche grazie allo sviluppo di certi strumenti tecnologici? SI forse è così, ma la risposta non mi sento di darla in termini definitivi, e non dimentico che in realtà il Giappone imperiale si arrese alla Russia e ai suoi fanti, non alle bombe atomiche americane. Su questi temi ci sono molti miti, e mi permetta invece un paio di osservazioni "laterali".

Prego la ascolto…

La prima: oggi siamo spiati in continuazione; ciò ci rende sicuramente meno liberi, ma molti ritengono che questo sia il *prezzo per la sicurezza* (i talebani hanno preparato bene il terreno, peraltro). Io non sono d'accordo, e tremo a pensare quante volte nella storia abbiamo già visto – e vedremo - che non le informazioni, ma la mano chi le gestiva, hanno causato distruzione. Se oggi si sia più liberi grazie alle spie digitali dovremmo chiederlo agli studenti di Hong Kong, chiedere loro perché si sono riversati su Telegram dell'esule Durov, abbandonando altri social network degli americani. Dovremmo chiederlo alle vittime del prossimo olocausto, che si consumerà grazie ai big data in poche ore: quello degli ebrei richiese qualche anno, poi in Ruanda in 100 giorni fecero fuori mezzo milione di persone, oggi grazie all'uso delle tecnologie digitali il prossimo genocidio si concluderà in poche ore – troveranno in un decimo di secondo figli, genitori e amici - e con qualche pennellata di fake news tutto sarà dimenticato dopo dieci twitter e quattro like.

Vero e inquietante… La seconda osservazione…?

Oggi le mamme hanno a disposizione dei magnifici guinzagli, corti e lunghi, dorati e leggeri, per tenere al laccio i loro figlioli. Le mamme dicono che sono più sicure, e i genitori sono "sicuri" o meglio sono "rassicurati". I figli sono più liberi? Vanno dove vogliono, trasgrediscono e imparano? No, nessuno oggi si sbuccia più le ginocchia. I figli stanno al guinzaglio e la sicurezza (dei genitori) è pagata con la moneta della libertà (dei figli). Ma tutto questo cosa comporta? Che i figli crescono in un ambiente protetto, hanno sempre a portata di un bottone cibo e riparo, nessuno gli parla delle cose brutte che potrebbero succedere, non fanno esperienza nel gestire esibizionisti, ladri e truffatori di strada, anzi in strada non ci vanno proprio mai, passano da una macchina a uno schermo, e … semplicemente NON crescono. Da grandi – ma quando saranno grandi? – non sapranno prendere una decisione – che sia politica, che sia di far un figlio, che sia di dire NO – e tantomeno sapranno combattere una guerra, essere solidali con gli altri, godere nell'aiutare il prossimo, crescere nella vera amicizia tra essere umani, nella tribù. Vorrei chiudere così: questo cattivo uso della tecnologia accompagnerà, accelerandola, una seria involuzione delle capacità umane in generale. Anche sul web, a proposito, la libertà la si conquista, non la si può ricevere in dono. Vale lo stesso per la sicurezza. Confido che i giovani sapranno conquistare l'una e l'altra. ■

Sloweb

MANIFESTO

Sloweb è un'associazione non profit fondata per promuovere l'uso responsabile degli strumenti informatici, del web e delle applicazioni Internet attraverso attività di informazione, educazione e lotta agli usi impropri da parte di organizzazioni di ogni natura.

Sloweb afferma che il web è uno straordinario mezzo di trasmissione del sapere, dei ricordi e delle informazioni di qualità. Sloweb riconosce le enormi opportunità ed il potenziale delle tecnologie digitali, anche per facilitare l'inclusione delle persone disabili.

Sloweb riconosce che l'uso delle tecnologie informatiche interferisce a fondo con la parte irrazionale, emotiva e inconscia della natura umana. Alle opportunità si affiancano quindi rischi e fenomeni sociali da valutare con attenzione e, in casi specifici, contrastare.

Sloweb si impegna a proteggere i diritti fondamentali anche sul terreno particolare della gestione ecologica dei dati digitali delle persone: ridurre, proteggere, selezionare, possedere, cancellare e gestire la propria eredità digitale.

Quanto sopra è essenziale per rendere il web più sicuro, libero e utile per tutti.

F5 Application Protection Report 2019: le applicazioni sono il nuovo campo di battaglia della sicurezza delle informazioni

Autore: **Paolo Arcagni,**
Systems Engineer Manager Italy & Malta di F5 Networks

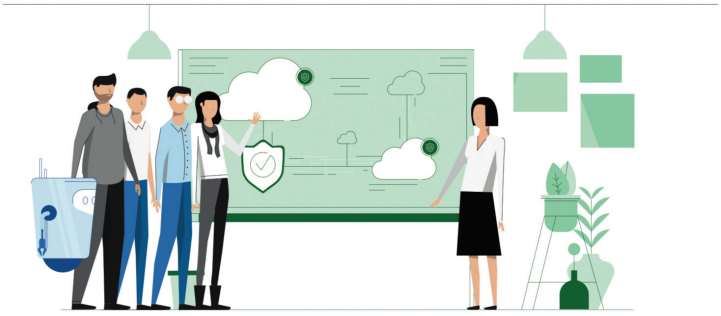
BIO

Da oltre 10 anni in F5 Networks, Paolo Arcagni ha iniziato il suo percorso professionale in azienda come Presales System Engineer, occupandosi dell'attività di prevendita per le soluzioni di Application Delivery Networking di F5. Nel 2010 è stato nominato System Engineer Leader Italy & Turkey fino all'attuale ruolo, che riveste da ottobre del 2012, di Systems Engineer Manager Italy & Malta, con responsabilità crescenti all'interno della Region. Paolo possiede un solido background tecnico e competenze specifiche nell'ambito del mercato dell'Application Delivery Networking con particolare preparazione rispetto a tematiche come il load balancing, l'ottimizzazione e la sicurezza applicativa. Con una laurea in fisica nucleare conseguita presso l'Università Statale di Milano, Paolo ha iniziato la sua carriera professionale in Vodafone come Business Analyst ed è stato System Engineer presso Centron International e Lucent Technologies.

Nei primi 30 anni di vita, Internet ha rappresentato principalmente un mezzo di trasmissione che permetteva agli utenti di spostare rapidamente le informazioni elaborate localmente in posizioni geograficamente diverse per ulteriori elaborazioni o utilizzi. L'archiviazione locale era ancora la norma e le informazioni trasmesse costituivano, nella maggior parte dei casi, un piccolo sottoinsieme di dati significativi che erano già stati visionati e analizzati dalle persone. C'erano alcune eccezioni ma, nella maggior parte dei casi, le informazioni che viaggiavano attraverso Internet restavano un piccolo sottoinsieme di un archivio più ampio di informazioni.

Negli ultimi 20 anni, Internet è cresciuto gradualmente diventando un luogo che contiene una percentuale sempre maggiore di tutte le informazioni disponibili e una piattaforma non solo di trasmissione ma anche di archiviazione ed elaborazione dei dati a qualsiasi livello di astrazione.

Una delle conseguenze interessanti è che il divario tra il software, che ha elaborato e archiviato le informazioni, e le reti, che le hanno trasmesse e visualizzate (spesso in file HTML statici che chiamiamo siti Web) è crollato. Praticamente tutto il software è ospitato online o ha bisogno di una connessione Internet per funzionare e gli utenti necessitano di connessioni Internet per aggiungere il contesto e il valore che trasforma i dati in informazioni. In questo mondo, tutte le applicazioni sono collegate in rete e tutte le reti terminano in applicazioni.



KEY FINDING 01

87% of respondents have multi-cloud architectures, driven by an app-first methodology.

L'applicazione oggi

Oggi le applicazioni sono il punto focale delle Operation moderne delle aziende private e, sempre più, anche delle organizzazioni non profit e del settore pubblico. Webmail, social media, motori di ricerca, servizi di online banking, prenotazione viaggi, database, streaming multimediale, eLearning e sistemi di gestione dei contenuti, che hanno sostituito i siti statici, sono tutti applicazioni. Come punto di incontro di utenti e reti, le applicazioni rappresentano il valore che definisce la maggior parte delle aziende e il punto di accesso a quello che gli aggressori apprezzano di più: i dati.

F5 ha scelto di focalizzarsi sulle applicazioni perché hanno inesorabilmente conquistato il centro della scena come componente determinante di Internet. Nell'ultima edizione del nostro *F5 Application Protection Report 2019* appare, infatti, evidente che l'unico obiettivo al quale gli aggressori danno più importanza delle applicazioni web sono gli utenti che si connettono a queste applicazioni, e che rappresentano il primo tassello per ottenere l'accesso ai dati.

L'evoluzione dei data breach e le principali minacce: il phishing sempre più protagonista

Uno dei capitoli più interessanti dell'analisi di quest'anno riguarda le tipologie di violazione dei dati che abbiamo affrontato esaminando i modelli dei diversi settori, le cause e le ripercussioni.

Nel 2018 avevamo esaminato 384 violazioni avvenute negli Stati Uniti nel 2017 in quattro stati: California, Idaho, Oregon e Washington. La maggior parte delle normative negli Stati Uniti richiedono che le vittime siano informate delle violazioni dei dati, ma al momento solo pochi procuratori hanno raccolto e condiviso pubblicamente le lettere sulla violazione sui propri siti Web. Poiché California, Washington, Idaho e Oregon rappresentano oltre il 16% della popolazione degli Stati Uniti, abbiamo ritenuto la dimensione del campione fosse sufficiente per consentirci di trarre alcune conclusioni interessanti. Nell'edizione di quest'anno abbiamo esteso la nostra analisi a 761 violazioni segnalate nel 2018 in 10 stati che rappresentano il 21,4% della popolazione degli Stati Uniti: California, Washington, Wisconsin, Vermont, New Hampshire, Iowa, Maryland, Oregon, Idaho e Delaware.

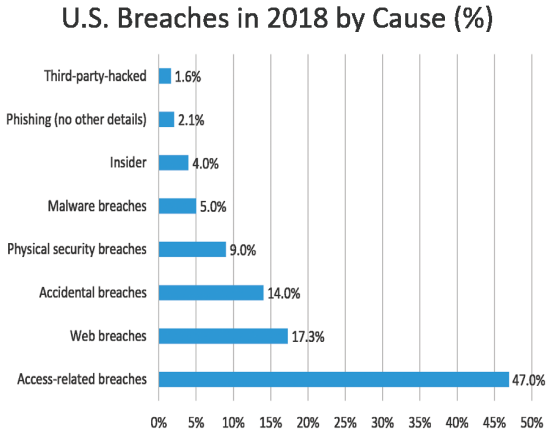
Nel 2018, avevamo identificato due principali vettori di attacco - l'**injection di codice tramite formjacking** e il **phishing**. In particolare, avevamo scoperto che lo skimming via injection delle carte di pagamento era la minaccia principale per le applicazioni. Si trattava di attacchi di injection che sfruttano le vulnerabilità delle applicazioni Web locali per caricare gli skimmer software delle carte di pagamento (a volte indicati nei report sulle violazioni come malware) in moduli di immissione dei pagamenti non sicuri. Gli attacchi di questo tipo rappresentavano il 21% di tutti i data breach analizzati e includevano molte delle violazioni basate su injection più significative avvenute durante il 2017. La maggior parte dei moduli di pagamento e delle applicazioni che gestivano "un carrello della spesa" compromesso erano eseguiti su PHP; inoltre, abbiamo scoperto che i tentativi di exploit PHP costituivano il 58% del traffico totale di attacco osservato dai sensori Loryka nel 2017.

Il phishing e altre tipologie di attacco al controllo degli accessi sono stati la seconda minaccia più significativa del 2018, rappresentando il 14% di tutte le violazioni analizzate. Nel corso del 2018 abbiamo scoperto che **le campagne di phishing si stavano trasformando, diventando più sofisticate e rilevanti**, quindi non ci ha sorpreso scoprire che, nel corso dell'ultimo anno, gli attacchi di phishing hanno effettivamente superato l'injection: il phishing è stato **responsabile del 21% delle violazioni avvenute nel 2018** con una causa nota, mentre l'injection per lo skimming delle carte di pagamento era responsabile di circa il 12%. Gli exploit e le tattiche specifiche possono cambiare leggermente, ma i due punti più deboli su Internet sono le persone e i moduli delle carte di pagamento basati su PHP - destinati a conservare il loro primato di vulnerabilità.

Primo passo: violare l'accesso

Le violazioni analizzate quest'anno dimostrano che gli esseri umani e le loro strutture di accesso continuano a essere uno dei punti più deboli delle applicazioni. Nel report di quest'anno, infatti, abbiamo riscontrato che la violazione dell'accesso rappresenta la percentuale più elevata tra le cause di violazione note, nel 47% dei casi.

Le sottocategorie all'interno della violazione dell'accesso sono molte e variegate, e comprendono il credential stuffing, il phishing per ottenere l'accesso alle credenziali di login, il brute forcing delle credenziali, e sono sostanzialmente tutte sono riconducibili a una forma di social engineering o al furto di credenziali. L'egemonia di queste tecniche rappresenta, in buona parte, un riflesso della forza di altri controlli tecnici:



perché se fosse più semplice aggirare completamente l'autenticazione, non vedremmo così tanti aggressori scegliere questa strada.

I principali target

Siamo stati in grado di raggruppare le violazioni identificando due target principali, che corrispondono alle due minacce più comuni: phishing e injection.

1 Le organizzazioni che accettano carte di pagamento sul Web

Queste aziende presentano un tasso elevato di compromissioni, avvenute con l'injection di moduli di pagamento. Il settore del commercio al dettaglio, che si basa fortemente sulle transazioni online, ad esempio ha registrato un tasso sproporzionatamente elevato di compromissioni tramite injection, con il 72% delle violazioni provenienti da questo vettore. Altre realtà simili, nel campo del manufacturing e delle tech, registrano violazioni di questo tipo sempre maggiori e anche il settore pubblico dimostra un'incidenza elevata di attacchi avvenuti con successo tramite injection, probabilmente a causa della prevalenza dell'exploit *Click2gov* che ha perseguitato le autonomie locali e i siti delle utility nel 2017 e nel 2018. In breve, per le organizzazioni che accettano carte di credito per il pagamento online, gli attacchi con injection delle forme di pagamento, come *Magecart*, rappresentano un rischio significativo.

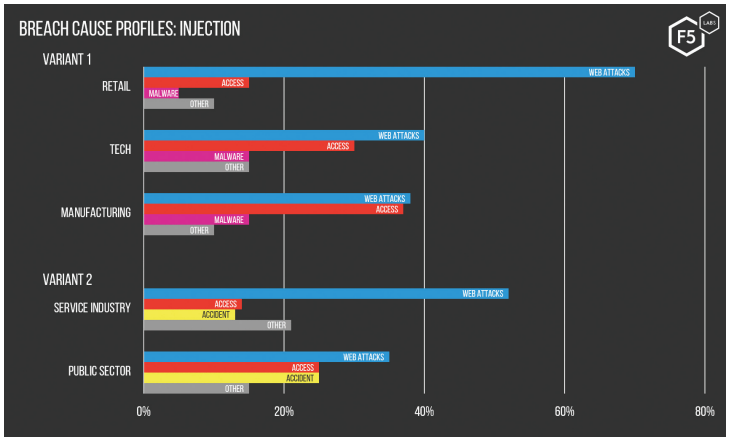


Figura 1: *Il grafico mostra i vari settori che hanno maggiori probabilità di subire una violazione dei dati attraverso l'injection e le variazioni della probabilità per il settore di queste violazioni nel tempo rispetto ad altre cause.*

2 Le organizzazioni che possiedono dati identificativi utilizzabili per le frodi

L'altro profilo a rischio che abbiamo identificato riguarda le organizzazioni dei settori finanziario, sanitario, educativo, no profit e amministrativo, che hanno una probabilità estremamente più elevata di essere compromesse attraverso il phishing o l'accesso illecito alla posta elettronica. Questo profilo si articola in modo diverso rispetto al secondo e il terzo vettore di violazione più frequente. Il malware e le minacce interne, ad esempio, svolgono un ruolo più importante nel settore contabile mentre gli incidenti o le violazioni fisiche hanno una prevalenza maggiore nella finanza, sanità, istruzione e non profit. Tuttavia, tutti questi settori mostrano una probabilità estremamente più elevata di subire attacchi di phishing o altre violazioni della posta elettronica.

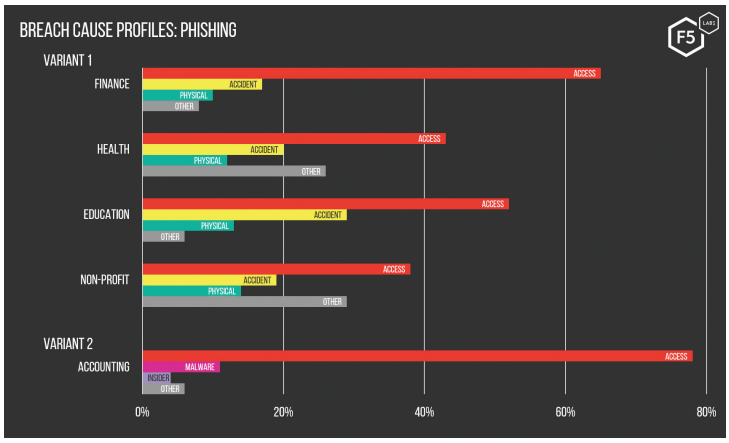


Figura 2: *Il grafico mostra i vari settori che hanno maggiori probabilità di subire una violazione dei dati attraverso il phishing e le sottili variazioni della probabilità che nel tempo avvengano violazioni tramite il phishing rispetto ad altre cause.*

In molti di questi casi, la lettera di notifica della violazione riportava come soggetti non autorizzati fossero stati in grado di sottrarre informazioni personali non crittografate all'interno delle cache di posta elettronica

dei membri dell'organizzazione, anche se la maggior parte delle aziende invita esplicitamente gli utenti a non archiviare informazioni sensibili nelle proprie caselle email, proprio per questo motivo.

I trend che abbiamo identificato sono significativi anche rispetto a come le organizzazioni dei diversi settori scelgono di conservare e trasmettere i propri asset più strategici. Quando il modello di business implica l'e-commerce, le stesse applicazioni di e-commerce rappresentano il percorso diretto verso l'obiettivo, senza presentare troppi ostacoli se non sono controllate correttamente. Non sorprende che le campagne Magecart all'inizio fossero dirette contro le vetrine Magento che funzionano su PHP, che, come abbiamo visto, continua a presentare una vulnerabilità preziosa per chi attacca.

Al contrario, le organizzazioni del secondo profilo, provenienti da settori come la finanza, l'healthcare e l'istruzione, possono archiviare le risorse sensibili lontano dai front-end web. Raggiungere gli obiettivi su tali reti di solito comporta attacchi complessi, a più fasi che richiedono un punto d'appoggio iniziale, che è quasi sempre offerto dal phishing e dalle violazioni dell'email. Sebbene sia certamente possibile trovare informazioni preziose nell'email, l'esfiltrazione di dati da fonti strutturate dall'uomo come l'e-mail è di solito laboriosa e vale la pena effettuarla solo per dati limitati e ricchi di valore, come proprietà intellettuali o comunicazioni politiche. Per attacchi su larga scala e orientati al profitto, l'e-mail rappresenta spesso solo il primo passo in una campagna più ampia per raccogliere informazioni personali (informazioni di identificazione personale), PHI (informazioni sanitarie protette) o PFI (informazioni finanziarie personali).

Conclusioni

I dati disponibili sulle violazioni ci offrono abbastanza elementi per concludere che il vettore di minaccia scelto da chi attaccherà dipenderà da dove e da come le organizzazioni hanno archiviato le risorse, obiettivo ultimo degli attacchi. Se, in virtù del loro modello di business, le organizzazioni orientate all'e-commerce devono archiviare PFI vicino ai propri front-end delle applicazioni, saranno proprio questi front-end a diventare il punto focale degli attacchi. Se le organizzazioni archivieranno i loro asset di valore altrove nelle reti, il social engineering e l'escalation dei privilegi saranno all'ordine del giorno, implicando quindi campagne di phishing.

Le applicazioni non sono solo il codice che eseguono, ma hanno a che fare con tutto ciò che le circonda che le fa nascere: architettura, configurazione, ulteriori risorse a cui l'applicazione si collega e, non ultimo i loro utenti. In altre parole, ci sono aspetti che hanno poco a che fare con la definizione ristretta di applicazione web, ma che possono avere enormi effetti sulla sicurezza di quell'applicazione.

La prevalenza di attacchi agli accessi, come il phishing, nei report sulle violazioni ci riporta a questo contesto più ampio segnalandoci la necessità di comprendere le applicazioni sia a livello dei singoli componenti che le compongono, sia a livello più ampio dell'intero ambiente in cui le persone le utilizzano.

Un'ultima riflessione che possiamo ricavare è che, nei vari settori di mercato presi in esame, le violazioni subite dalle aziende confermano il valore dei programmi di sicurezza basati sul rischio rispetto a quelli che impostati su best practice o checklist.

Sappiamo che gli attacchi che hanno avuto successo sono riusciti a tracciare con una certa precisione il punto in cui le organizzazioni avevano memorizzato il loro obiettivo, le risorse sensibili; ne consegue che le organizzazioni devono personalizzare i controlli e l'architettura rispetto alle minacce concrete che devono affrontare. Questo conferma una la nostra affermazione di lunga data: la valutazione del rischio deve rappresentare una pietra angolare di qualsiasi programma di sicurezza e il primo passo in qualsiasi risk assessment è un processo di inventario sostanziale e continuo. ■

Social media e schermi cambiano il cervello?

Il Convegno internazionale organizzato dall'Osservatorio Tuttimedia – Media Duemila, si è svolto a Roma presso la FIEG

Autore: **Massimiliano Cannata**

Siamo nell'era delle tecnosfide, che si stanno giocando su due grandi versanti: il primo è quello delle competenze e della modifica sostanziale di alcune fondamentali funzioni cognitive, che incidono sulle relazioni interpersonali, sull'apprendimento e sul comportamento; il secondo attiene, in particolare, alla ridefinizione del rapporto tra stato e mercato, sulla scia del progressivo tramonto del Leviatano e del nuovo ruolo che il settore pubblico e le istituzioni dovranno ritrovare nella società complessa. L'evento organizzato **dall'OTM (Osservatorio Tuttimedia) e da Media Duemila**, che si è svolto a Roma presso la FIEG (Federazione Italiana Editori e Giornali) sul tema: *Social media e schermi cambiano il cervello?* va collocato nel primo grande filone di analisi.

Il confronto tra esperti, neuroscienziati e studiosi del comportamento ha assunto l'originale modalità di un Atelier, costruito sull'intuizione di **Derrick de Kerckhove** (docente presso il Politecnico di Milano e direttore scientifico Tutti Media/Media Duemila) allievo di **Mc Luhan** tra i massimi esperti al mondo di nuovi media, teorizzatore dell'intelligenza connettiva, quale irrinunciabile antidoto contro il dilagare della superficialità e dell'ignoranza. "E' importante *proporre concrete azioni di policy che pongano l'essere umano al centro, al fine di dare impulso a una scienza dei comportamenti sociali e a una conoscenza della rete che porti ad agire su viral comunication, no-critical interaction, hate speech, troll e fake news"* – spiega **Maria Pia Rossignaud**, Direttrice TuttiMedia/MediaDuemila, giornalista esperta di innovazione, da sempre attenta osservatrice delle fenomenologie del cambiamento.

L'interrogativo lanciato da OTM e da Media Duemila merita grande attenzione. La rivoluzione digitale ha generato un salto "epistemologico", ha modificando le categorie stesse della conoscenza, spazio e tempo non sono più le forme a priori kantiane delle nostre sensazioni, siamo, insomma, un passo oltre, dobbiamo imparare a fare i conti con una trasformazione tutta da studiare e soprattutto da capire. A scanso di equivoci è giusto ricordare, come ha fatto molto efficacemente **Vittorino Andreoli** nel suo ultimo saggio (L'uomo col cervello in tasca, ed. Solferino) che la macchina cerebrale umana e la macchina digitale rimangono entità fortunatamente diverse. Il nostro cervello, che rimane la cifra superiore della nostra identità di soggetti pensanti, si è evoluto in tempi molto lunghi, pensare che l'uso continuo dei pc e dello *smartphone* possa modificare la struttura profonda del cervello potrebbe essere fuorviante, tuttavia non può certo essere sottovalutata la sollecitazione esercitata dall'utilizzazione continua di questi nuovi strumenti sulla plasticità neuronale, con conseguenze sul linguaggio, sui modi di relazionarsi, sui livelli di concentrazione. "Come studiosi – puntualizza de Kerckhove - abbiamo il dovere di dare suggerimenti basati su analisi concrete per almeno provare a limitare gli effetti negativi che l'uso intensivo della rete provoca non solo nei giovani. Negli ultimi anni, infatti, alcuni comportamenti si sono diffusi in differenti fasce della popolazione diventando strutturali. Sarà lo schermo che dona l'illusione dell'invisibilità, che induce a comportamenti estremi ?".

La "narcosi" da schermo

La domanda dello studioso, che rimette in gioco il problema della verità come valore, concetto impegnativo che avevamo smarrito per strada, è di quelle destinate a non trovare risposta definitiva. Nello schermo diventiamo vittima di una "narcosi della luce - come ha scritto **Donatella Di Cesare** (cfr. *Sulla vocazione politica della filosofia*, ed. Bollati Boringhieri) - che ci porta a negare l'altro, in una sorta di immanenza satura. Dimentichiamo che senza l'alterità non può esserci pensiero critico, non sarebbe nemmeno nata la filosofia. Usiamo lo schermo

come maschera, decidendo di giocare sulla finzione, con tutte le conseguenze del caso". Siamo di fronte ai sintomi di un disagio, che ci fa comprendere come sia arrivato il momento di trovare un bilanciamento tra reale e virtuale, che potrebbe aiutarci a ridurre lo spazio per la "bugia semiologica", che è l'anticamera della falsificazione che ha alimentato il potente motore delle *fake news*, con il suo pericoloso alone di verità creata in cui stiamo tutti correndo il rischio di affogare.

Non si può, comunque, parlare a nessun livello di evoluzione, senza fare darwinianamente riferimento al peso dell'ambiente sulla maturazione della civiltà. Il contesto entro cui ci muoviamo ha assunto le connotazioni dell'infosfera (la fortunata definizione è di **Luciano Floridi**, *La quarta rivoluzione, ed. Raffaello Cortina*), che è uno "spazio ibridato" in cui non è più possibile fare la differenza tra *on line* e *off line*. La vecchia idea per cui si andava nel *cyber spazio* per collegarsi e poi ci si disconnetteva per tornare "sulla terra" è ormai superata. *Onlife* è la cifra dell'io nella social society, bisogna partire da questa consapevolezza per tracciare le prossime tappe dello sviluppo umano. Ne è convinto **Roberto Saracco** (EIT Digital): il nostro cervello – ha commentato nel corso del dibattito - si è evoluto attraverso processi di selezione in modo da consentire la risposta più efficace all'ambiente. All'aumentare della complessità i nostri cervelli riescono anche a immaginare, cioè a proiettarsi in una dimensione ipotetica, che potremmo definire virtuale, che li porta a esaminare il risultato di azioni. Questo apprendimento si traduce in conoscenza in parte esplicita trasmissibile col linguaggio, in parte implicita. La seconda non passa attraverso il linguaggio, ma attraverso l'esperienza del singolo e l'apprendimento per prova ed errori". La grande abilità acquisita dai nativi digitali a usare smartphone e pc, cosa di cui gli adulti non sono certo capaci, prova la validità del ragionamento di Saracco, aprendo ulteriori pesanti interrogativi, che riguardano la fragile triangolarità costituita dal rapporto tra: mente, cervello e linguaggio. L'avvento dei social ha fatto maturare un "secondo tempo" di Internet, esponendoci, infatti, a un sistema di "echi" che amplifica un vuoto di significati, ma anche di senso, che si traduce in un pericoloso smarrimento psicologico ed esistenziale.

I paradossi della società della conoscenza

I sintomi della malattia, analizzati dagli studiosi, hanno tante sembianze. Le tracce sono molteplici. La più stretta attualità ce ne fa individuare una che ci conduce fino all'esito dei testi Invalsi che stanno sollevando un ampio dibattito sui giornali. Un numero enorme di nostri ragazzi non è capace di comprendere un testo in lingua italiana. Siamo probabilmente tornati analfabeti. Da *sapiens sapiens* l'uomo di oggi tende a trasformarsi in *"stupidus stupidus"*, facile preda di nuove solitudini. Il pericolo che si profila è quello di non parlare più, arriveremo a quello che molti studiosi a partire dal già citato Andreoli definiscono come una sorta di autismo digitale, un universo chiuso, popolato da tante monadi che non comunicano. L'uso del Pc rafforza questa tendenza alla schematizzazione: utilizziamo il ditino in su se qualcosa piace e in giù quando non piace. A dominare è la logica binaria, non più la logica razionale che, almeno da Aristotele in poi, è posta a fondamento del pensiero e della civiltà occidentale.

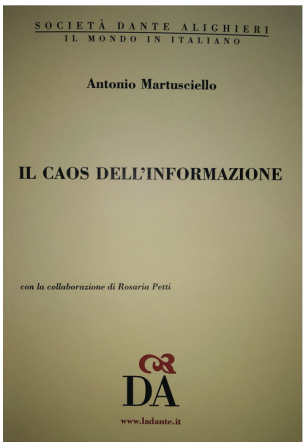
Siamo di fronte a uno dei tanti "paradossi della società della conoscenza", come li chiamerebbe uno dei più grandi pensatori viventi quale **Michel Serres**, che, cosa ancora più grave, può avere delle ripercussioni sulla qualità della democrazia. "Le società nelle quali prevalgono le asserzioni vuote di significato – fa opportunamente notare lo scrittore ed ex parlamentare e magistrato **Gianrico Carofiglio** – sono quelle in cui i politici non hanno percezioni dei doveri e dell'uso del linguaggio. Tutto questo contrasta con l'etica civile di uno stato democrarito".

Ritornando a Serres, nel suo agile pamphlet *Non è un mondo per vecchi* il filosofo francese ricorre all'immagine tratta dagli *Essais* di **Michel de Montaigne** che racconta del martirio di San Dionigi, che pur decapitato cammina con la testa sotto il braccio fino alla chiesa di Saint-Denis, posta sulla sommità di Montmartre che ne eternerà il sacrificio. Alla generazione del "pollice" sta accadendo un fenomeno simile: ha delegato a PC, Smartphone e tablet le funzioni superiori tipicamente umane, come la memoria, l'immaginazione e la capacità di ragionamento. I giovani hanno "messo" letteralmente in tasca le facoltà cerebrali, le hanno riposte nello zaino, magari nel cellulare; salvo ogni tanto, come fanno i bambini a scuola mentre il maestro/professore spiega, accendere lo strumento per cercare risposte alla nostra curiosità.

Le perplessità di Serres sono un'ulteriore dimostrazione di come siamo solo all'inizio della rivoluzione, i ragazzi non hanno più la stessa testa, non abitano il nostro spazio cognitivo, è cambiato il linguaggio, oltre alla percezione della fatica e del lavoro. Probabilmente solo ora stiamo cominciando a capire che la tecnologia non basta, la vera sfida si giocherà su contenuti e la capacità autentica di fare qualità e di innovare.

Se l'incontro ha avuto un *primum movens* generato da un colloquio tra lo stesso de Kerckhove e **Roberto Viola**, direttore DG Connect della Commissione europea su *Hate speech*, notizie false e comportamenti antisociali, alla luce delle tante questioni aperte sarà bene andare avanti. La riflessione su questi delicati aspetti avrà bisogno del tempo lungo di una ricerca seria, che auspicabilmente dovrà coinvolgere anche le élite politiche e le classi dirigenti imprenditoriali non sempre preparate ad affrontare i ritmi di una trasformazione che sta cambiando la nostra postura rispetto alla realtà e agli eventi della storia contemporanea. La buona notizia sta nel fatto che le indicazioni e i risultati dell'incontro in FIEG saranno oggetto di una convention internazionale già prevista, che si terrà sempre a Roma, nel prossimo ottobre in collaborazione con DG Connect. ■

IL CAOS DELL'INFORMAZIONE



Il tema della qualità dell'informazione e della diffusione "democratica" delle notizie è una delle grandi questioni del nostro tempo, che non può essere sottovalutata o derubricata nei titoli di coda di qualche notiziario, magari programmato negli orari del palinsesto notturno. Come dimostrano i puntuali rilevamenti dell'osservatorio sui TG dell'Eurispes che si riferiscono alle ultime elezioni europee, è risultato molto basso, se non addirittura trascurabile, lo spazio dedicato a programmi e ai progetti politici da cui dipenderà il futuro del Continente, mentre si perdono spazi e tempi preziosi che vengono dedicati ad affrontare superficiali gossip, finalizzati alla disinformazione di massa. Evidentemente un *vulnus* esiste nel mondo dell'informazione, come viene ben delineato da un agile e illuminante saggio di ***Antonio Martusciello*** Commissario dell'Autorità Garante delle Comunicazioni, già Parlamentare con una importante esperienza nel settore dei media, realizzato con la collaborazione del Consigliere Giuridico ***Rosaria Petti*** (***Il caos dell'informazione***, *ed. Società Dante Alighieri)*. Se, infatti, "la rivoluzione tecnologica con i suoi linguaggi e i suoi codici ha assunto un ruolo sempre più determinante", come viene fatto correttamente notare dagli autori nell'introduzione, il prepotente sviluppo di strumenti e apparti hi-tech non ha purtroppo trovato corrispondenza nell'eguale maturazione di un assetto di sistema dei media, che attualmente non appare in grado di tutelare né gli utenti, che si muovono nel mare aperto dell'informazione pervasiva, né tanto meno le aziende editoriali, che dovrebbero sentire la responsabilità di confezionare notizie attendibili, utilizzando sempre con rigore e serietà di metodo le fonti.

Nel breve excursus che apre la trattazione vengono richiamate alcune tappe essenziali che hanno segnato il progresso dell'umanità e che hanno avuto un epicentro significativo proprio nelle modalità di elaborazione, costruzione e trasmissione del sapere. Nel XV secolo l'Europa passa dalla tradizione orale alla stampa, il salto di paradigma non poteva essere più radicale, cambiano equilibri e convinzioni diffuse, muta l'assetto stesso dell'uomo rispetto al mondo che lo circonda, sino a trasformare convinzioni religiose e filosofiche, che sembravano immutabili. Quello che si consuma nella modernità è una rivoluzione epistemologica destinata a pesare per sempre sul ruolo stesso dell'uomo nel cosmo.

Altro salto di paradigma importante è segnato dalla comunicazione elettronica e dall'avvento della TV. Il politologo Giovanni Sartori parlerà di passaggio *dall'homo sapiens, all'homo videns*, al di là della brillante definizione, occorre porre attenzione al capovolgimento del punto di vista, causato dal nuovo elettrodomestico, che entra nelle case di tutti. Una rivoluzione di codici e linguaggi anche in questo caso, imperniata non più sul segno - significante della parola e della proposizione articolata - quanto sull'immagine. Nazareno Taddei, teologo di *Civiltà Cattolica* tra i massimi esperti di cultura cinematografica, aveva definito la civiltà della TV come fondata sul "linguaggio contornuale", cioè su una specifica sintassi dell'immagine che ha le sue regole, i suoi tempi, il suo particolare modo di arrivare nella mente e nel cuore dell'utente. Il legislatore lo aveva capito in tempo, come dimostra la direttiva CEE correttamente richiamata nella trattazione, che si preoccupava di fissare logiche e obiettivi cui le emittenti televisive, che dalla fine degli anni settanta stavano proliferando in tutta Europa, erano obbligate ad attenersi: fornire programmi ai cittadini col *"fine di informare, intrattenere, istruire".*

Tre verbi pesanti, che dovrebbero almeno in teoria riassumere il senso della deontologia professionale per gli operatori dell'informazione. Oggi, purtroppo, viene quasi da sorridere se, anche per un attimo, ci si sofferma a pensare all'uso che viene fatto di un mezzo straordinario e potente come la televisione, che ha determinato storicamente, basti pensare all'opera di pionieri come Alberto Manzi con il suo *Non è mai troppo tardi*, la prima grande alfabetizzazione di un popolo, come quello italiano, che negli anni Cinquanta era ancora in larga parte ignorante, che viveva tra mille incertezze il contesto di una nazione ancora prostata dalle atrocità della guerra.

Verso il citizen journalism

Il passato non ritorna, per fortuna, ma la forza dei principi non dovrebbe mai essere rimossa. Con l'avvento della Rete, arriviamo così al cuore dello studio di Martusciello, la sintassi della comunicazione muta ancora. Il consumatore diventa un attore, nasce il *citizen journalism* tutti possono partecipare alla costruzione delle notizie. La libertà di accesso esalta potenzialmente tutti, come osserva puntualmente l'autore, peccato però che non coincida con l'articolazione di un'offerta armoniosa, né tanto meno con adeguate garanzie per gli utenti e nemmeno per le aziende editoriali, spiazzate da un mercato dell'informazione che in poco tempo ha cambiato profondamente le sue dinamiche.

C'è a questo punto da chiedersi: Il modello industriale che si sta facendo strada sarà in grado di garantire quel diritto all'informazione iscritto nella nostra Costituzione, senza intaccare la sfera della riservatezza e della privacy? La domanda è destinata a rimanere senza risposta, mentre un nuovo potere si fa strada: quello dell'algoritmo, che come ha argomentato molto bene Michele Mezza in un suo recente lavoro esprime *"la potenza del calcolo tra dominio e conflitto"* (*cfr. Algoritmi di libertà* ed. Donzelli).

Per capire lo scenario che abbiamo davanti basti pensare che ogni giorno reti e sistemi di connettività raccolgono alcuni *exabyte* di informazioni un valore pari alla sesta potenza di mille, un miliardo di miliardi. Sono numeri da farebbero impallidire anche la biblioteca di Alessandria. In un intero anno la raccolta di dati in termini di durata potrebbe equivalere a 36mila anni di video in HD, come se avessimo a disposizione una pila composta da 250 miliardi di DVD. In una realtà datificata ridotta a stringhe e a bit orientarsi non è certo semplice, immersi come siamo nella dimensione dell'"infosfera". Su una popolazione di circa sette miliardi di persone, sono più di 4 miliardi gli utenti connessi, mentre la data economy è stata attualmente valutata in Europa per un valore annuo di 60 miliardi di euro. E' il mito del calcolo che prende sempre più corpo.

Algoritmo è, infatti, la parola chiave di questa delicata fase dello sviluppo scientifico e tecnologico, perché entra nella politica, nell'economia, nell'informazione, nell'impresa. 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 gli individui della facoltà di scelta e di decisione, processi che non appaiono più frutto di valutazioni culturali, maturate con l'esercizio dello studio e della riflessione.

Siamo tutti propensi a prendere sempre più fiduciosi il mare aperto della rete per consultare una "Sibilla" che però non sarà poi così sincera come ci aspetteremmo. Il medium digitale alimentato da una particolare ermeneutica applicata ai big data, tende a fornire delle risposte che rispondono a logiche economiche e di mercato non sempre trasparenti. La potenza di strumenti in grado di autocorreggersi, di migliorare la performance, di replicare (pensiamo all'IA e al *Machine Learning*) modalità di ragionamento della "mente" umana, apre un fronte delicatissimo di riflessione sul rapporto uomo macchina, etica e sviluppo della scienza.

Il dato come asset sociale

Va detto che ormai nella società dell'informazione il dato si è tramutato in un asset sociale. L'algoritmo assume e licenzia (si potrebbero richiamare tanti casi eclatanti), la *blockchain* automatizza le organizzazioni e può fare a meno di sindacati, partiti, istituzioni. Se applichiamo tutto questo al mondo dell'informazione, come fa molto opportunamente Antonio Martusciello in questo scritto, ci accorgiamo di quanto gravi siano le implicazioni sul terreno della qualità democratica. Pochi grandi player sono in grado di gestire l'enorme patrimonio di dati; la "macchina" della notizia, non è più quella dei giornali, con il risultato che i cosiddetti *over the top* che operano in rete monopolizzano pesantemente gli utenti, condizionando il mercato.

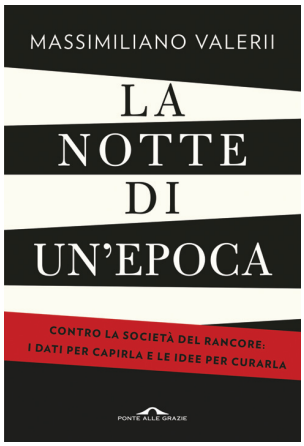
Il palinsesto informativo è nelle mani di pochi, i social network aggregano news, i giornali sono divenuti soggetti passivi, intermediati dagli algoritmi. Il mondo insomma appare capovolto. Il 54% degli italiani acquisisce il grosso delle notizie attraverso strumenti governati da algoritmi, con l'aggravante che, come rivela uno studio britannico, l'utente che frequenta i social per acquisire notizie, non ricorda quasi mai il *news brand* titolare delle informazioni.

Altro risvolto sollevato dallo studio, ma questo richiederebbe una trattazione a sé, riguarda la crescente dicotomia stato/piattaforme. Stiamo assistendo a un indebolimento della sovranità nazionale insieme e a uno svuotamento dei parlamenti (il dibattito sulla democrazia diretta sollevato da molti studiosi è significativo) 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, potrebbe portare in breve tempo a un mutamento della fisionomia dello stato liberale, che credevamo fosse, almeno da Locke in poi, immodificabile. Detto in sintesi: la digitalizzazione di tutti i processi sociali è destinata a trasformare il profilo, i soggetti e i linguaggi non solo dell'informazione ma anche della politica.

Come si vede di questioni aperte ce ne sono molte, per altro amplificate da sistemi per definizione complessi, come quelli che abitiamo. Il ruolo delle Authority e delle politiche pubbliche sarà molto importante. Il saggio, di cui stiamo parlando, proviene dallo studio di un Commissario dell'AGCOM ed è un segnale importante ed estremamente positivo. Serviranno sempre di più d'ora in avanti appropriate iniziative legislative volte a tutelare i diritti fondamentali e le libertà conquistate in anni di sofferenza e di conflitti. Nello stesso tempo bisognerà rafforzare la qualità delle classi dirigenti e la cultura di cui devono farsi portatrici. Una cosa va sempre ribadita: lo straordinario sviluppo della scienza e della tecnologia non deve essere imbrigliato certo, ma non può neanche cogliere impreparati i cittadini e gli stati.

Ricordiamoci che la buona informazione è il sale di ogni democrazia liberale, i diritti sono le palafitte su cui si regge la civile convivenza, la scuola e l'istruzione il carburante attraverso cui far crescere cittadini adulti e consapevoli, in grado di tramutare il caos dell'informazione, nell'ordinata architettura di un sapere condiviso, che potrà finalmente aprire, al di là di ogni falsa retorica, la strada di un autentico progresso. Speriamo che chi ci governa, a tutti i livelli, sappia tenere a mente questa elementare verità. ■

LA NOTTE DI UN'EPOCA



Il saggio di Massimiliano Valerii, filosofo e direttore generale del Censis comincia offrendo al lettore una grande suggestione. A Treviri nel maggio nel 1968 ***Ernst Bloch***, in un'aula gremita di giovani studenti, pronuncia il discorso di commemorazione di ***Karl Marx*** nella giornata del centocinquantesimo anniversario della sua nascita. Il suo intervento è un elogio della dignità e della speranza, che occorre difendere e coltivare se vogliamo avere un posto nel mondo. Con parole che affascinano il grande pensatore si rivolge all'uditorio in estasi: "dobbiamo camminare eretti, quel camminare che non ancora si ha in senso giusto". Il riflesso potente delle considerazioni di Bloch si proietta su un'attualità che vede l'individuo sofferente, troppo spesso schiacciato nella sua libertà di pensiero e di azione. "Bloch – spiega Valerii - è l'uomo che mette al centro della storia la forza dell'immaginario. Nella sua filosofia la speranza è il fondamento ontologico dell'esistenza. Egli si è contrapposto alla corrente fredda del marxismo tutta economicismo, una corrente calda fatta di umanesimo reale". A dispetto del "declinismo" imperante, si può provare a invertire la rotta. "Siamo baciati dall'infinito dobbiamo solo averne consapevolezza, per spezzare le tenebre della notte di un'epoca e riconquistare un lembo di futuro". La scintilla prometeica che può squarciare le tenebre è la filosofia a porgerla, una terapia dell'anima e della mente che dobbiamo tornare a praticare.

Evidentemente nella società del rischio, per usare una definizione di Beck non solo è lecito, ma addirittura risulta necessario sognare. "La crisi che stiamo vivendo ha un fondamento materiale, strutturale: il blocco dei processi di mobilità sociale ascensionale – prosegue lo studioso - L'ascensore sociale si è inceppato: scende, ma non sale. Si è rotto cioè il patto sociale che aveva guidato il nostro sviluppo dal dopoguerra in avanti, per oltre mezzo secolo. La tacita promessa per cui generazione dopo generazione si sarebbero migliorate le condizioni di benessere

materiale". Ma la crisi ha anche una base immateriale, non meno importante se pensiamo al naufragio delle tre grandi narrazioni entro le quali l'Occidente aveva provato a costruire la sua identità. Il sogno di trovare una nuova patria in una Europa unita senza più frontiere, mentre poi c'è stata l'Europa matrigna dell'austerity e la Brexit. L'apologia della globalizzazione, mentre poi abbiamo scoperto i *forgotten men* di Trump. La convinzione che Internet e la rivoluzione digitale avrebbero diffuso conoscenza e democrazia ai quattro angoli del pianeta, mentre oggi parliamo di *fake news*, censura e propaganda sul web". Il risultato è un enorme spaesamento, cui occorre porre rimedio. La filosofia, tornare a ragionare in una società travolta dalla fretta e dalla superficialità può essere una chiave importante per ritrovare il "filo del discorso". Valerii crede profondamente alla funzione di una disciplina che per troppo tempo era stata relegata a un ruolo di secondo piano, soprattutto nella fase della grande euforia tecnologica che tendeva a innalzare i profili tecnici e gli studi di matrice ingegneristica. La filosofia, per dirla con le stesse parole dell'autore può essere un ***antidoto per guarire dalla terribile "deflazione delle aspettative"***. Quando il disordine e lo smarrimento prendono il sopravvento, per cercare risposte si ricorre non a caso ai classici. Hanno il pregio di poter essere letti e riletti continuamente, perché hanno qualcosa da dire in ogni epoca e non esauriscono la loro capacità di influenza. Le loro pagine ingialliscono, ma non invecchiano, e si rivelano sorprendenti soprattutto nei tempi di crisi. Brillano nel buio, rischiarano le ombre". Nel testo probabilmente per questo viene riproposta la rilettura di alcuni grandi riferimenti del pensiero, il tutto è giocato non in maniera sistematica, ma per balzi e suggestioni. Il lettore può trarre ispirazione da queste sollecitazioni, per uscire dall'oscurità e vedere lo stato delle cose sotto un cono di luce che possa profilare nettamente le sagome che al momento appaiono tutte sfocate.

"Grande è la ricchezza di un'epoca in agonia"

Non va neanche sottovalutata la complessità di questa fase storica, perché può essere foriera di positività oltre ogni aspettativa. *"Grande è la ricchezza di un'epoca in agonia"*, aveva scritto Bloch. Aggiungeva poi che l'uomo non vive di solo pane, soprattutto quando non ne ha. Quando il pane scarseggia, materialmente e metaforicamente, proprio nelle situazioni di grave crisi, gli uomini consumano più immaginario. Significa che è proprio nelle fasi più difficili che la fantasia non deve essere sottoalimentata di immagini e simboli. *Siamo di fronte a una nuova frattura della storia. L'auspicio dell'autore, che facciamo nostro è quello di tornare a camminare eretti, "perché l'infinito è in noi"*. Le giovani generazioni, spesso ignorate e sottovalutate dalla politica, anche per motivi quantitativi, possono riuscire a far proprio questo stimolo e a modificare un assetto di sistema che sottovaluta le intelligenze e i talenti. "So bene – scrive nelle pagine conclusive l'autore - che oggi il ventaglio delle opportunità esistenziali dei giovani si è molto ristretto. E so bene anche che il futuro spesso ci inganna, ci seduce e poi ci tradisce, perché i sogni possono rivelarsi delle chimere e i desideri non avverarsi. Ma a loro vorrei raccomandare di non perdere l'ardore di futuro. Per curare l'inquietudine collettiva e l'insoddisfazione personale abbiamo bisogno di un progetto di redenzione: di fare qualcosa che ci migliori e ci renda più soddisfatti di noi stessi. È questa la molla per dispiegarsi nel futuro". ■

FORMAZIONE, COMPETENZA E LINGUAGGI ADEGUATI PER UNA SICUREZZA 4.0

Massimo Butti si occupa di ICT, organizzazione e normativa dai primi anni 80, con particolare riferimento alle tematiche di Sicurezza, della Privacy e dell'Audit aziendale. Mandando in libreria *Sicurezza Totale 4.0 l'ABC sulla physical Cyber Security per i DPO e le PMI (e non solo) edizioni Iter*, si può dire che fa un grande regalo ad addetti ai lavori e non. Il saggio, giunto alla seconda edizione, è uno strumento utile, non solo per i manager della sicurezza e i professionisti del settore, ma anche dirigenti e funzionari responsabili di diverse aree organizzative che hanno tra gli obiettivi quello di proteggere gli asset aziendali, dovrebbero tenersi ben stretto nella cassetta degli attrezzi.

Il volume pur essendo ponderoso, risulta molto agile e di facile lettura, apprezzabile è lo sforzo di divulgazione compiuto dall'autore, che con grande padronanza attraversa questioni che oggi sono di vilate importanza per la vita di istituzioni e imprese. *"Lo spirito di fondo che ha ispirato il mio lavoro fin dalla prima edizione – spiega Butti – è connotato da una constatazione molto semplice: vi sono molti DPO che hanno competenze legali e non sempre il corredo di conoscenze necessarie in ambito ICT, Sicurezza e Audit. Occorreva dunque colmare questo gap cercando di far parlare questi due mondi"*. Una ricerca dunque quella di Butti, che non ha solo un lato squisitamente tecnico, perché attiene all'individuazione di un codice di comunicazione condiviso che deve essere utilizzato in una duplice direzione. Sono, infatti, tanti i profili tecnici che operano in azienda ad aver bisogno di misurarsi con gli amministratori delegati e più in generale con i responsabili di diverse aree aziendali. *"Le parole per dirlo"* sono perciò un bene inestimabile, come sosteneva *Wittgenstein*: "il "mio linguaggio è il mio mondo", privati del linguaggio si finisce con l'essere ingoiato in un solipsismo inguaribile". Il tema è affascinante e non riguarda solo gli appassionati di filosofia del linguaggio, se si considera il livello di complessità che caratterizza il contesto sociale e ambientale in cui oggi siamo immersi. Una pletora di norme non sempre comprensibili, sopravanzate dalla progressione di un'evoluzione tecnologica che non ha mai avuto ritmi così serrati, obbliga tutti ad aggiornare continuamente competenze e linguaggi. Far parlare gli *"specialismi"* sarà dunque la sfida del prossimo futuro. Butti è giù dentro questa sfida, come dimostrano ampiamente le sue ultime pubblicazioni, fondate su un concetto forte di *cross – competence*, che vuol dire innanzi tutto collocarsi sul fronte di chi vuole scongiurare l'incomunicabilità, fonte non solo di equivoci, ma sovente di grande spreco economico e di tempo per le aziende.

Il saggio originale nell'impianto presenta diversi livelli di lettura, risultando un'originale sintesi tra il manuale tradizionale e un iper testo, che rimanda continuamente ad un apparato sitografico e bibliografico molto ricco e soprattutto utile. In virtù di questo particolare impianto il target si rivolge a un pubblico vasto, che va dai consulenti, ai manager, agli esperti in senso generico, fino ai neofiti che sono interessati a conoscere un universo di problematiche in futuro destinate ad assumere una centralità sempre più forte sia in ambito istituzionale che imprenditoriale. "Sono molteplici le risorse e le fonti aperte – precisa l'autore – che gratuitamente possono essere consultate dai manager

della security della grandi aziende ma soprattutto delle PMI che hanno necessità di aggiornarsi sulle novità normative e nel contempo di implementare soluzioni di sicurezza efficienti sul piano dei costi ed efficaci sul terreno della performance. Ritengo sia un peccato non sfruttare questo serbatoio a disposizione di tutti".

La prima parte del libro si squaderna dinanzi al lettore nelle sembianze di un'interessante *overview* sugli "ecosistemi della sicurezza", con una serie di capitoli descrittivi e didattici che fanno vedere il processo di valutazione del rischio sia dal punto di vista dei beni aziendali, sia dal punto di vista dell'evoluzione della normativa privacy, con particolare riferimento alle tematiche relative alla tutela dei diritti e delle libertà fondamentali delle persone fisiche. Via via che si entra dentro le questioni, il passo della trattazione assume le sembianze dell'approfondimento. Le sezioni dedicate agli asset da proteggere e alla gestione del rischio, in cui vengono prese in esame le tipologie più diffuse di minaccia e le vulnerabilità che mettono a rischio la *business continuity* delle grandi come delle piccole imprese, sono da approcciare con attenzione, per le tante informazioni utili che ogni lettore può trarne per farne tesoro nel lavoro quotidiano.

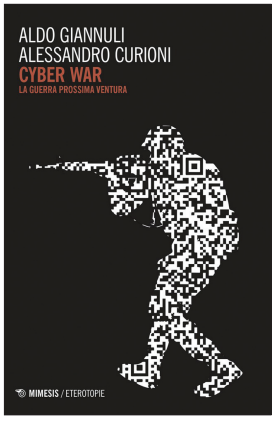
Il capitolo dedicato agli scenari operativi apre il versante più "pragmatico" della trattazione. "Ho cercato di dare delle risposte – commenta Butti – alla molteplicità delle richieste cui i manager della sicurezza e i responsabili DPO devono far fronte per implementare le policy, per innalzare un sistema che sia adeguato alla protezione degli *asset* e per elaborare un metodo di analisi del rischio che possa essere all'altezza dei nuovi scenari evolutivi dell'ICT".

Nell'epoca dei BIG Data, degli algoritmi, dell'IOT la sicurezza assume una valenza strategica. L'approccio che oggi viene richiesto comporta una concezione *by design* della *security* capace di mettere in fila i temi della Privacy, (crf. hendbook del Garante dedicato al GDPR, il D.lgs. 196/03) l'evoluzione degli apparati e dell'intero ecosistema della sicurezza che stanno mutando concezione e architettura, sulla spinta della rivoluzione digitale.

In conclusione pare opportuno richiamare Gabriele Faggioli, Presidente di Clusit che ha scritto nella presentazione alla seconda edizione: *"…Il libro di Giancarlo Butti, viene incontro a una precisa esigenza di formazione multidisciplinare e di una maggiore cultura per tutti… Ci sarà chi si troverà più a proprio agio nel capitolo inerente la normativa applicabile, chi magari ha già conoscenza delle misure di sicurezza logiche o della gestione del rischio. Il libro ha il grande pregio di proporre, per i non specialisti, una visione a 360 gradi".* Proprio per questa apertura che non è solo teoretica, ma culturale e più in generale di metodo, che fa da contraltare ai tanti tentativi di affermazione di un "pensiero unico" oggi molto in voga, credo bisogna ringraziare l'autore. ■

SCENARI DI GEOPOLITICA: LA CYBER WAR PROSSIMA VENTURA

C'è una guerra silenziosa alle porte che nessuno può permettersi di sottovalutare, sarà combattuta con armi invisibili, schieramenti fluidi, in "trincee virtuali". Aldo Giannuli storico, collaboratore di procure e commissioni d'inchiesta sulle stragi di Stato e Alessandro Curioni, giornalista specializzato in cybersicurezza autore di numerosi interessanti saggi sul tema (Come pesci nella rete, La privacy vi salverà la vita, Questa casa non è un hashtag, per ricordare i più recenti n.d.r) con Cyber War, la guerra prossima ventura (Mimesis edizioni) introducono il lettore in uno scenario complesso, poco conosciuto nelle dinamiche e perciò di difficile interpretazione. Dobbiamo prepararci al peggio? "Occorre tenere conto



– spiega Curioni - che siamo di fronte alla possibile prospettiva che da qui a pochi anni si verificherà la madre di tutte le guerre asimmetriche. E' facile immaginare quali sarebbero gli obiettivi degli aggressori, che molto probabilmente saranno tutte le infrastrutture critiche destinate a erogare servizi essenziali dai trasporti, all'energia, fino all'acqua potabile. Se fosse vero, sul fronte dei difensori si schiererebbero i civili". A chi strabuzza gli occhi perché sorpreso, lo stesso autore risponde senza tentennamenti: proprio così, la prima linea di difesa sarebbe rappresentata dal personale destinato a gestire la sicurezza dei sistemi di decine di grandi aziende. Per fare un paragone sarebbe come se durante la Prima Guerra Mondiale a respingere gli austro-ungarici sul Piave ci fossero stati i dipendenti della FIAT, della Pirelli, della Montecatini guidati dai rispettivi dirigenti". I protagonisti di questa nuova forma di conflitto, gli obiettivi della conquista e soprattutto le strategie che vengono messe in campo per contrastarli non hanno nulla a che vedere con l'impostazione militare tradizionale. Nazioni Stati Uniti, Russia, Cina e Corea del Nord e Iran sono quelle più avanti in termini organizzativi e tecnologici. Se l'obiettivo, come in qualsiasi guerra, è quello di piegare il nemico alla propria volontà, l'aggressore punta a quelle che oggi si definiscono infrastrutture critiche e va detto che a differenza dei conflitti convenzionale tutti i vantaggi sono ascrivibili all'attaccante. "Volendosi anche porre dal lato della vittima il fronte da proteggere sembra essere infinito, se pensiamo all'interconnessione tecnologica tra le organizzazioni strategiche e i loro partner. Volendo penetrare i sistemi del principale operatore energetico di un paese, molto probabilmente il primo e silenzioso attacco sarebbe indirizzato al più oscuro dei suoi fornitori. Inutile sottolineare che un problema come quello classico della logistica risulta irrilevante: non ci sono, infatti, soldati da nutrire e mezzi da rifornire dispersi su migliaia di chilometri di fronte. In definitiva il difensore potrebbe essere costretto a ricorrere a una "difesa in profondità": aggredire a sua volta il nemico costringendolo a rimediare ai danni che subisce, cosa che ne rallenta l'azione".

Sono particolarmente temibili le armi segrete messe in campo dai cyber guerrieri. Il genere più numeroso è indubbiamente rappresentato da quelli che comunemente sono definiti malware, ovvero software che compromettono o danneggiano il normale funzionamento di un sistema o delle informazioni che esso gestisce ed elabora. La storia ne ha mostrati decine con diverse caratteristiche. Tuttavia la peculiarità delle armi cyber è la relazione molto stretta con l'obiettivo. Per fare un paragone con il mondo reale si può immaginare una guerra in cui per distruggere ogni singola tipologia di struttura sia necessario costruire uno specifico missile. L'indissolubile rapporto che nel cyber, lega arma e obiettivo viene definito dal termine vulnerabilità, cioè l'esistenza di una o più debolezze o errori che possano essere sfruttate per ottenere il risultato atteso. Le armi segrete sono quelle basate sulle vulnerabilità cosiddette "zero day", ovvero ancora sconosciute. La nuova corsa agli armamenti è proprio quella alla ricerca di queste debolezze.

L'attualità dello studio è ampiamente dimostrata dalla cronaca, che riferisce sempre più spesso di attacchi informatici portati al cuore di reti e sistemi informativi e di banche dati di rilevanza strategica. Gli stessi equilibri economici e politici, sono condizionati da questa nuova forma di "pirateria" che a differenza

delle compagnie di ventura che mettevano a ferro e fuoco le città del tardo Medioevo al loro passaggio, si insinuano nei canali digitali violando la riservatezza che nel passato custodiva quei "segreti", che sono il cuore di ogni compagine statale. Il caso delle recenti elezioni americane, richiamato nel saggio, è molto indicativo. Di particolare interesse la differenza, introdotta nel testo, tra due tipologie di conflitto: "info war e cyber war". La prima è la naturale evoluzione di quella che un tempo veniva chiamata "Guerra Fredda", quello del "Russiagate" è un esempio di scuola che si inscrive in questa precisa fenomenologia, che vede i social network al centro della scena in quanto strumenti eccezionali di propaganda, capaci di influenzare l'opinione pubblica con precisione chirurgica. Al contrario il conflitto cyber sposta il baricentro dell'attenzione verso altri contesti. "L'etimologia di cyber si riferisce alla costruzione di macchine in grado di riprodurre le funzioni del cervello umano e più in generale a sistemi capaci di autoregolarsi attraverso input e output di comando e di controllo idonei a sviluppare alti livelli di automazione, finalizzate a svolgere attività complesse. Trattando di questa seconda fenomenologia è più corretto parlare di attacchi rivolti a oggetti smart, al mondo IoT e a quello delle Intelligenze artificiali. In particolare data la natura di questi oggetti un vero conflitto cyber dovrebbe produrre effetti "diretti" nel mondo reale. La compromissione di un sistema che gestisce il controllo dei voli di un aeroporto potrebbe facilmente e direttamente uccidere delle persone, un attacco a un sistema di posta elettronica difficilmente potrebbe ottenere lo stesso risultato e di certo non in modo diretto".

E' evidente che in questo "cambiamento d'epoca" si sta consumando un "salto di paradigma" anche nel modo di concepire e attuare i conflitti. Chi opera nella sicurezza a tutti i livelli dovrà tenere conto che la logica del "controllo" legata alla vecchia concezione dei perimetri fisici da presidiare alla governance del rischio. Il risultato è che avremo bisogno di aggiornare conoscenze e competenze per reggere la sfida portata da livelli crescenti di complessità. "Dobbiamo avere la consapevolezza – scrivono gli autori - che le nuove tecnologie presentano dei vantaggi e che i rischi sono direttamente proporzionali a questi vantaggi. Se le tecnologie penetrano il mondo reale e ne gestiscono in modo autonomo i mezzi e gli strumenti dobbiamo comprendere che tutte le minacce che abbiamo sempre pensato fossero confinate al di là di un schermo, da domani saranno "applicabili" al mondo reale, con tutto quello che ne consegue.

Infine non è certo esercizio fine a se stesso chiedersi come l'Italia si colloca nel nuovo scacchiere internazionale che vede la potenza tecnologica e le competenze informatiche asset strategici ineludibili attraverso cui, finita l'epoca del Leviatano, si potrà esercitare una nuova forma di egemonia su popoli e Continenti. "In Italia siamo piuttosto indietro – è il parere di Curioni - ma c'è un'altra fondamentale considerazione di carattere generale da fare. La pervasività delle tecnologie dell'informazione nei paesi più evoluti e anche dotati di maggiori risorse non solo militari, li renderà sempre più vulnerabili a una guerra cyber e questo potrebbe rappresentare l'unica possibilità per tutte quelle organizzazioni incapaci di contrappore al nemico un arsenale adeguato per una guerra convenzionale. Consideriamo che un singolo missile intelligente "Cruise" può costare un milione di dollari per ogni pezzo, un malware pochi spiccioli. Nel nuovo scenario che abbiamo tratteggiato nel saggio si capisce molto bene come anche le organizzazioni "povere", avranno la capacità di concentrare le proprie risorse per sferrare un contrattacco al cuore delle reti. Di certo si tratta di un'opportunità più unica che rara, perché sarebbero in grado di colpire l'avversario sul suo territorio. Come reagirebbe l'opinione pubblica alla privazione di un bene essenziale come l'energia elettrica? L'interrogativo finale lanciato dallo studioso genera un brivido dietro la schiena, riportandoci a scene già viste, concepite da menti criminali, responsabili di aver generato quel clima di terrore, diventato purtroppo cifra essenziale di quella "società del rischio" che il grande sociologo tedesco Ulrich Beck aveva per primo intuito e descritto. ■

Recensioni bibliografiche: Massimiliano Cannata

Una pubblicazione

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:
Viale Europa 175 - 00144 Roma, Italia
Tel: 06 59582272
info@gcsec.org
Şcoala de Înot nr.18, 550005,
Sibiu, Romania

www.gcsec.org
www.cybersecuritytrends.ro
www.swissacademy.eu
www.cybertrends.it

CERT STAR

Il CERT STAR è un programma di incontri a porte chiuse dedicato ai CERT e ai SOC italiani volto ad alimentare le competenze, promuovere la cooperazione e la condivisione di esperienze. Nel corso degli incontri sono analizzate a livello tecnico operativo le principali tematiche "core" dei team di security.

GLOBAL CYBER SECURITY CENTER

- 28 febbraio APT e Cyber Range
- 04 aprile Dark Web Intelligence
- 10 luglio Cyber Threat Intelligence
- 19 settembre Application Security
- 07 novembre End Point Security
- 03 dicembre Incontro Executive

Per maggiori informazioni scrivere a
info@gcsec.org

brinthesis

Carbon Black.

f5

FORTINET

INTSIGHTS
Defend Forward.

XM CYBER

Il primo Tool per valutare il livello di maturità del tuo CERT e dei suoi Servizi

Available Soon

www.certrating.it

Per maggiori dettagli
Info@gcsec.org