Cybersecurity Trends

Edizione italiana, N. 2 / 2024

INTERVISTE VIP:

- MARCO LA ROSA
- FRANCO PIZZETTI

ISSN 2559 - 1797
ISSN-L 2559 - 1797

Folder centrale: NIS2, Cybersecurity e Cyber-resilienza

Cybersecurity Trends

Leggi la rivista **online** quando
e dove vuoi!
Puoi scegliere tra news, articoli,
interviste, nuove sezioni,
approfondimenti,
rubriche e contenuti multimediali.

Scopri anche la nuova sezione
dedicata agli esperti della cyber security!
Al suo interno
Hacking Around e Technical Video.

Nella sezione Rubriche:
Bibliografia
Dalla Redazione
Dalle Aziende
Dalle Università
Eventi
Offerte di Lavoro

www.cybertrends.it

Indice

Editoriale

2 **Una nuova sfida per la Sicurezza Informatica in Europa.**
Autore: Nicola Sotira

Folder Centrale – NIS2, Cybersecurity e Cyber-resilienza

3 **Cambiamenti Normativi: Quando il Breaking Bad è Buono.**
Autore: Jelena Zelenovic Matone

8 **La Direttiva NIS2: un'opportunità per elevare il livello di cyber security del Paese.**
Autore: Rossella Macinante

11 **NIS, NIS2, Golden Power e perimetro di Sicurezza Cibernetica Nazionale.**
Autore: Corradino Corradi

15 **Compliance europea alle porte per la resilienza delle imprese italiane.**
Autore: Elena Vaciago

18 **Le sfide delle Academy e le Risorse Umane nella Cyber Security aziendale.**
Autore: Italo Piroddi

20 **Direttiva NIS2: le sfide per le imprese italiane.**
Autori: Lorenzo Russo e Franceso Binaschi

23 **Il processo di attuazione della NIS 2 in Italia.**
Autore: Erik Longo

Interviste VIP

26 **Difendiamo il pluralismo delle narrazioni per ricostruire i "sentieri interrotti". Intervista VIP con Marco La Rosa.**
Autore: Massimiliano Cannata

28 **La regolazione della società digitale, pilastro della Costituzione europea. Intervista VIP con Franco Pizzetti.**
Autore: Massimiliano Cannata

Focus

31 **Dalla Direttiva al Comportamento: NIS 2 e Psicologia nell'Era Digitale.**
Autore: Veronica Patron

Bibliografia

32 **Roberto Mania, Capitalisti silenziosi - Egea Ed.**
Autore: Massimiliano Cannata

32 **Biagino Costanzo,Il cigno è grigio - Rubbettino ed.**
Autore: Massimiliano Cannata

33 **XIX Rapporto Censis sulla comunicazione - Ed. Franco Angeli.**
Autore: Massimiliano Cannata

34 **Andy Greenberg,Tracers in the dark, Randome Houseed.**
Autore: Massimiliano Cannata

Una nuova sfida per la Sicurezza Informatica in Europa.

Autore: Nicola Sotira

L'evoluzione del panorama delle minacce informatiche e l'importanza crescente delle infrastrutture digitali hanno spinto l'Unione Europea ad aggiornare la sua direttiva sulla sicurezza delle reti e dei sistemi informativi. La nuova Direttiva NIS2 (Network and Information Systems Directive 2) rappresenta un significativo passo avanti rispetto alla versione precedente, introducendo una serie di misure e requisiti volti a rafforzare la resilienza cibernetica delle infrastrutture critiche. La prima Direttiva NIS stabiliva un quadro normativo atto a migliorare la sicurezza delle reti e dei sistemi informativi in tutta l'Unione Europea. Tuttavia, l'evoluzione rapida delle minacce informatiche e le lacune emerse nell'implementazione della direttiva hanno evidenziato la necessità di un aggiornamento. La NIS2 è stata concepita per affrontare queste sfide, ampliando il campo di applicazione e introducendo requisiti più stringenti.

Punti caratterizzanti la NIS2:

Ampliamento del Campo di Applicazione

La NIS2 estende il campo di applicazione rispetto alla precedente direttiva, includendo un maggior numero di settori critici. Oltre ai settori tradizionali come energia, trasporti, sanità e finanza, la NIS2 copre ora anche le infrastrutture digitali, le amministrazioni pubbliche e altri settori chiave.

Armonizzazione

Una delle principali critiche alla prima Direttiva NIS riguardava l'implementazione disomogenea tra gli Stati membri. La NIS2 mira a risolvere questo problema promuovendo una maggiore armonizzazione delle misure di sicurezza e dei requisiti di segnalazione degli incidenti.

Sicurezza e Gestione del Rischio

La direttiva introduce requisiti di sicurezza più rigorosi per le organizzazioni, obbligandole a implementare misure tecniche e organizzative adeguate per gestire i rischi informatici. Questo include la necessità di effettuare valutazioni del rischio regolari, adottare misure di sicurezza adeguate e garantire la continuità operativa.

Segnalazione degli Incidenti

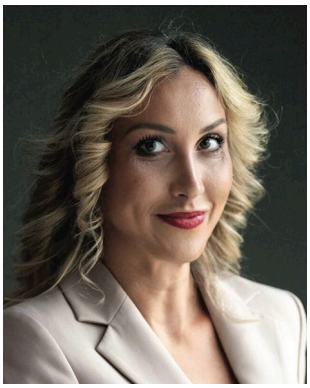
La nuova direttiva richiede alle organizzazioni di segnalare gli incidenti di sicurezza significativi entro 24 ore dalla loro scoperta. Questo è un cambiamento significativo rispetto ai tempi di segnalazione più lunghi previsti dalla NIS1, con l'obiettivo di migliorare la risposta rapida agli incidenti e la condivisione delle informazioni.

L'implementazione della NIS2 comporta diverse sfide per le organizzazioni. In primo luogo, queste devono rivedere e migliorare le loro pratiche di sicurezza informatica per soddisfare i nuovi requisiti. Questo può richiedere investimenti significativi in tecnologie di sicurezza, formazione del personale e aggiornamento delle politiche di gestione del rischio. Inoltre, le organizzazioni devono essere pronte a segnalare tempestivamente gli incidenti di sicurezza, il che implica la necessità di sistemi efficaci di rilevamento e risposta agli incidenti. La cooperazione e la condivisione delle informazioni con le autorità competenti diventano essenziali per migliorare la resilienza collettiva contro le minacce informatiche. La NIS2, al di là delle sue sfide rappresenta un passo importante verso una maggiore sicurezza delle reti e dei sistemi informativi in Europa. Rafforzando i requisiti di sicurezza e migliorando la cooperazione tra gli Stati membri, la nuova direttiva mira a creare un ambiente digitale più sicuro e resiliente. Le organizzazioni devono prepararsi adeguatamente per conformarsi ai nuovi requisiti, adottando un approccio proattivo alla gestione del rischio e alla sicurezza informatica. ■

BIO

Nicola Sotira è 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.

Cambiamenti Normativi: Quando il Breaking Bad è Buono.



Autore: Jelena Zelenovic Matone

Introduzione:

Di pari passo con la continua evoluzione del mondo digitale, anche le sfide e le minacce che le organizzazioni si trovano ad affrontare sono in continuo aumento, in particolare nel settore finanziario. In risposta ai crescenti rischi legati alle minacce informatiche e alle interruzioni operative, l'Unione Europea (UE) ha introdotto il Digital Operational Resilience Act (DORA). Questa importante normativa mira a istituire un quadro normativo unificato, volto a rafforzare la sicurezza delle reti e dei sistemi informativi delle istituzioni finanziarie che operano all'interno dell'UE.

Il Regolamento DORA introduce una nuova era di controlli normativi, obbligando le istituzioni finanziarie a rafforzare le proprie difese contro una vasta gamma di interruzioni e minacce legate all'ICT. Tuttavia, ciò che distingue il regolamento DORA è il suo approccio proattivo ai test di resilienza digitale. In sostanza, DORA incoraggia le organizzazioni ad adottare una mentalità da "breaking bad", in cui l'hacking etico, ovvero testare volontariamente la propria organizzazione alla ricerca di vulnerabilità, non è solo accettabile ma anche raccomandato.

Questo cambiamento di mentalità segna un superamento dei paradigmi normativi tradizionali, in cui l'importanza era data principalmente alla conformità e alle misure reattive. Al contrario, DORA sostiene una posizione proattiva, incoraggiando le organizzazioni ad anticipare, prepararsi e mitigare le potenziali minacce informatiche prima che si concretizzino.

L'ethical hacking, o il penetration testing, è una pietra miliare del framework di test di resilienza digitale del DORA. Attraverso la simulazione delle minacce e delle vulnerabilità informatiche del mondo reale, le organizzazioni possono identificare i punti deboli dei loro sistemi e di

BIO

Rispettata leader CISO, insignita del CISO dell'anno per il 2019 in Lussemburgo, Sentinel CISO Global 2020, EU CISO 2020 e Ambasciatore dell'anno 2021 in Lussemburgo, Jelena è esperta di Cybersecurity versatile e innovativa con enfasi sulla gestione del rischio di sicurezza informatica/ risk management, creazione di policy e procedure, sicurezza IT/ IS, operazioni IT, audit, mitigazione del rischio, miglioramento dei processi aziendali, governance IT, business process improvement, IT governance. Appassionata di partecipazione e incoraggiamento delle donne alla cybersecurity e ai programmi STEM. Prima del ruolo attuale, ha ricoperto il ruolo di Senior Operational Risk e ISO manager per un'altra istituzione dell'UE. All'inizio della carriera, ha gestito IT Audit and Compliance per Sobey's, uno dei due rivenditori nazionali di generi alimentari in Canada e Audit, Corporate Development, M&A e strategie di crescita e IT Audit per George Weston, una delle più grandi società di trasformazione e distribuzione degli alimenti in Canada quotata in borsa.

conseguenza rafforzare le loro difese. Questo approccio proattivo non solo migliora la postura di cybersecurity di un'organizzazione, ma promuove anche una cultura di miglioramento continuo e di innovazione.

Mentre il regolamento DORA si profila all'orizzonte, le organizzazioni devono prepararsi a un cambiamento radicale dei requisiti normativi. La conformità non è più sufficiente; la resilienza è fondamentale. Adottando i principi dell'hacking etico e dei test di resilienza digitale, le organizzazioni possono affrontare le complessità del DORA con fiducia, sapendo di essere protette da un panorama di minacce in continua evoluzione.

DORA

Il Digital Operational Resilience Act (DORA) è un'importante normativa introdotta dall'Unione Europea per migliorare la resilienza del settore finanziario contro le minacce informatiche e i malfunzionamenti operativi. Rappresenta un quadro completo per affrontare le crescenti sfide poste dagli attacchi informatici, garantendo la stabilità e la sicurezza dei servizi finanziari nell'era digitale.

DORA comporterà senza dubbio un cambiamento di paradigma nel panorama della cybersecurity e della resilienza operativa per le imprese e le istituzioni finanziarie che operano nell'UE. Ecco come influirà su di loro:

Maggiore Controllo Normativo: DORA imporrà un controllo normativo più severo, richiedendo alle istituzioni finanziarie di soddisfare standard più elevati di cybersicurezza e resilienza operativa. Ciò comporterà requisiti di reporting e misure di conformità più rigorosi.

Focus sulla Cybersecurity e sull' IT Risk Management: Il Regolamento sottolinea l'importanza della cybersecurity e della gestione del rischio informatico, richiedendo alle organizzazioni di implementare misure solide per identificare, proteggere, rilevare, rispondere e recuperare dalle minacce informatiche e dalle interruzioni operative.

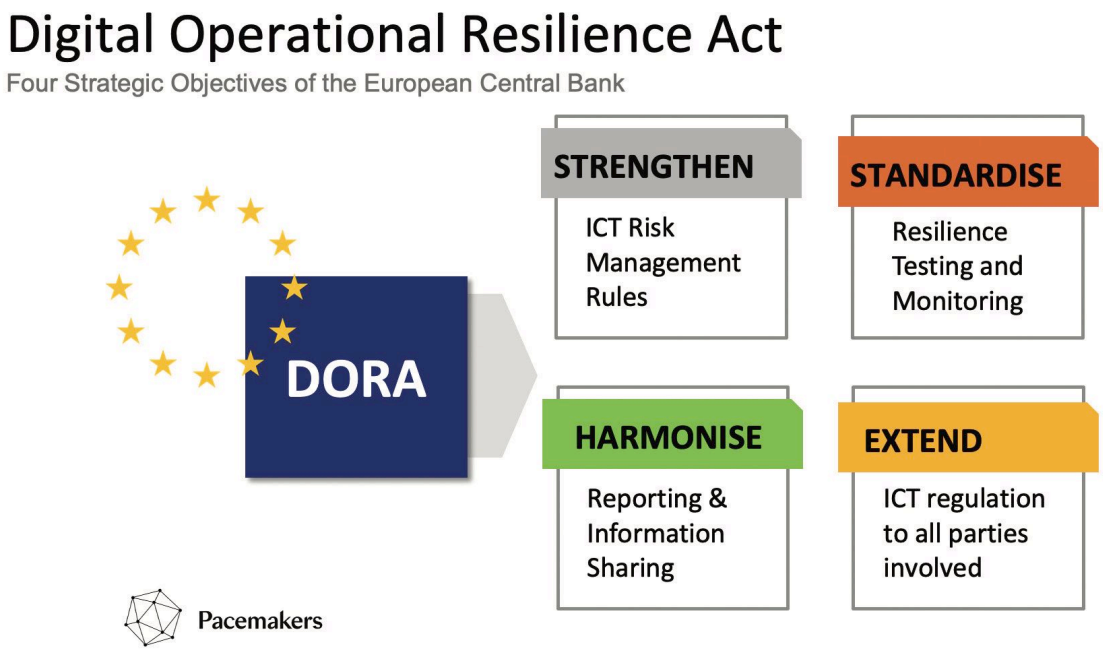
Maggiore Responsabilità e Trasparenza: DORA prevede che i dirigenti e i membri del consiglio di amministrazione abbiano la responsabilità di garantire la resilienza delle loro organizzazioni. Promuove una maggiore trasparenza sugli incidenti informatici e impone alle aziende di notificare tempestivamente alle autorità competenti le interruzioni gravi.

Collaborazione e Information Sharing: Il Regolamento incoraggia la collaborazione e la condivisione delle informazioni tra istituzioni finanziarie, autorità di regolamentazione e altre parti interessate per migliorare la resilienza collettiva contro le minacce informatiche.

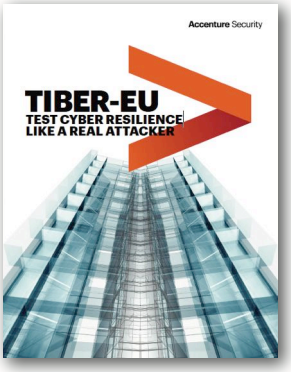
Sanzioni per la Non-Compliance: La mancata conformità al DORA potrebbe comportare gravi sanzioni, tra cui multe e danni alla reputazione, spingendo così le organizzazioni a dare priorità alla cybersecurity e alla resilienza operativa.

I cinque pillar più importanti del DORA possono essere sintetizzati come segue:

- Incident Reporting and Management: Stabilire procedure chiare per la segnalazione e la gestione degli incidenti informatici in modo tempestivo ed efficace.
- ICT Third-Party Risk Management: Implementazione di misure solide per valutare e gestire i rischi associati a fornitori di servizi e fornitori di terzi parti.
- ICT Operational Resilience: Garantire il funzionamento continuo dei sistemi e dei servizi critici delle tecnologie dell'informazione e della comunicazione (ICT).
- ICT Security: Rafforzare le misure di cybersecurity per proteggere da accessi non autorizzati, violazioni dei dati e altre minacce informatiche.
- Overarching Governance and Management Arrangements: Implementare solide disposizioni di governance e gestione per supervisionare e garantire l'efficacia delle misure di resilienza operativa.



Come il quadro TIBER-EU può aiutare a raggiungere gli obiettivi del DORA:



Il framework TIBER dell'Unione Europea (Threat Intelligence-Based Ethical Red Teaming) può svolgere un ruolo fondamentale nell'aiutare le organizzazioni a soddisfare i requisiti del DORA, in particolare nei test di resilienza informatica. TIBER fornisce un approccio standardizzato per condurre simulazioni controllate di attacchi informatici, note come esercitazioni di red teaming, per valutare l'efficacia delle difese di sicurezza informatica e delle capacità di risposta agli incidenti di un'organizzazione. Simulando scenari di attacco e di minacce informatiche reali, TIBER consente alle organizzazioni di identificare le vulnerabilità, testare la propria resilienza e migliorare la propria postura di cybersecurity.

L'iniziativa Threat Intelligence-Based Ethical Red Teaming for the European Union (TIBER-EU) è uno strumento fondamentale nell'arsenale delle difese di cybersecurity, in particolare nel settore finanziario. Progettato per rafforzare la resilienza informatica, TIBER-EU fornisce un quadro standardizzato per la conduzione di simulazioni controllate di attacchi informatici, comunemente chiamate esercitazioni di red teaming.

Il concetto centrale, TIBER-EU mira a replicare minacce informatiche e scenari di attacco reali, consentendo alle organizzazioni di valutare l'efficacia delle loro difese di sicurezza informatica e delle loro capacità di risposta agli incidenti. Sfruttando le informazioni sulle minacce e utilizzando tecniche di ethical hacking, TIBER-EU permette alle istituzioni finanziarie di identificare le vulnerabilità, testare la propria resilienza e rafforzare le difese contro le minacce informatiche.

I vantaggi di TIBER-EU sono numerosi, soprattutto nel contesto del Digital Operational Resilience Act (DORA) introdotto dall'Unione Europea. Ecco alcuni vantaggi principali:

Risk Assessment Completo: TIBER-EU consente una valutazione completa della postura di cybersecurity di un'organizzazione attraverso la simulazione di minacce informatiche sofisticate. Identificando le vulnerabilità e i punti deboli, le istituzioni finanziarie possono stabilire le priorità delle azioni di rimedio e destinare le risorse per mitigare i rischi in modo efficace.

Miglioramento delle Capacità di Incident Response: Attraverso le esercitazioni di red teaming, TIBER-EU consente alle organizzazioni di valutare e perfezionare le proprie capacità di risposta agli incidenti. Simulando gli attacchi informatici in un ambiente controllato, le istituzioni finanziarie possono identificare le falle nelle loro procedure di risposta e perfezionare i processi di gestione degli incidenti per ridurre al minimo l'impatto degli incidenti informatici del mondo reale.

Conformità Normativa: TIBER-EU si uniforma strettamente agli obiettivi del DORA, che impone solide misure di cybersecurity e test di resilienza digitale nel settore finanziario. Conducendo le esercitazioni TIBER-EU, le organizzazioni possono dimostrare la conformità ai requisiti del DORA e migliorare la propria conformità alle normative.

Rafforzamento della Fiducia degli Stakeholder: Testando e convalidando in modo proattivo le proprie difese di cybersecurity attraverso TIBER-EU, le istituzioni finanziarie possono rafforzare la fiducia degli stakeholder, tra cui clienti, investitori e autorità di regolamentazione. Dimostrare un impegno per la resilienza informatica, può rafforzare la fiducia e la reputazione in un contesto finanziario sempre più digitalizzato.

Miglioramento Continuo: TIBER-EU promuove una cultura del miglioramento continuo, fornendo alle organizzazioni preziose informazioni sulle minacce informatiche emergenti e sull'evoluzione delle tecniche di attacco. Integrando le lezioni apprese dalle esercitazioni di red teaming, le istituzioni finanziarie possono perfezionare le loro strategie di cybersecurity e avere un notevole vantaggio difensivo rispetto agli attaccanti cyber.

Automazione:

Anche l'automazione svolge un ruolo fondamentale nel migliorare la resilienza operativa e l'efficacia della cybersecurity. Gli strumenti automatizzati possono facilitare le attività di gestione ordinaria, migliorare i tempi di risposta e aumentare l'efficacia nel rilevare e mitigare le minacce informatiche. L'automazione può

anche facilitare il monitoraggio e la valutazione continua dei sistemi ICT, consentendo alle organizzazioni di identificare e risolvere in modo proattivo le vulnerabilità prima che possano essere sfruttate dagli aggressori.

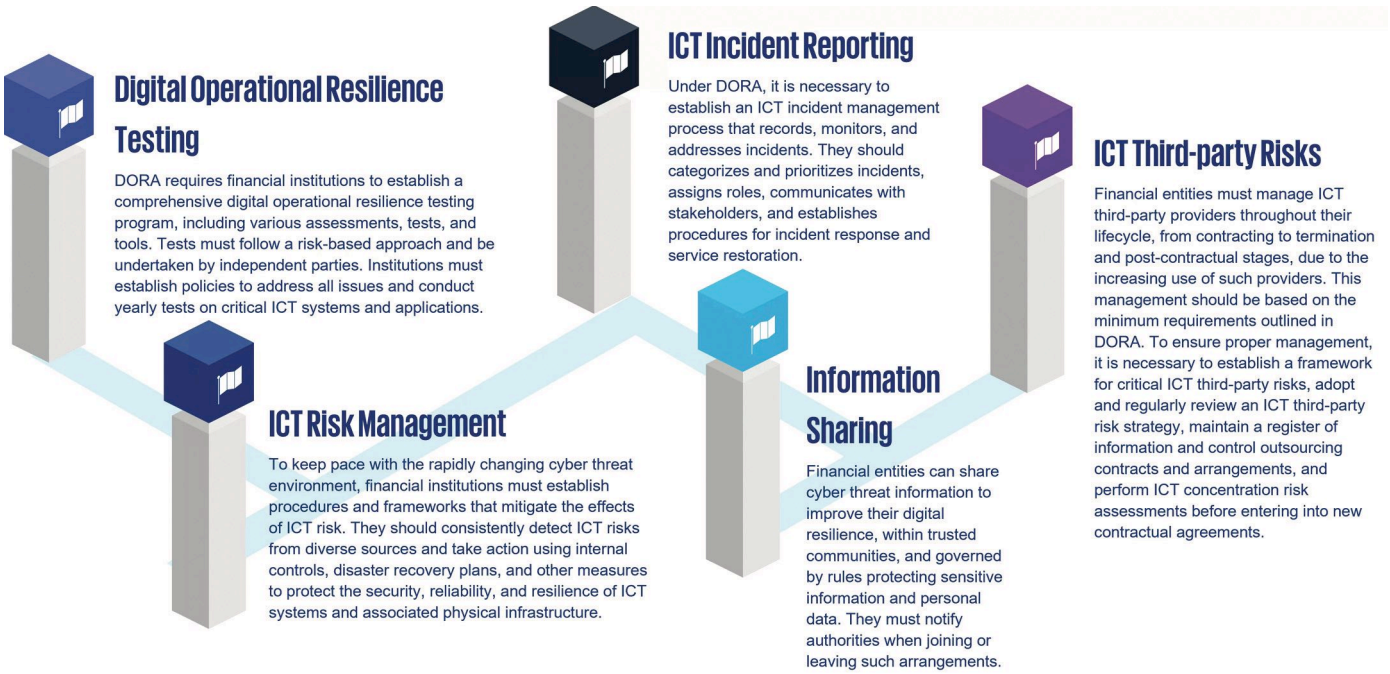
Uno di questi tool automatizzati è la piattaforma di test DDoS (Distributed Denial of Service) di Mazebolt, che aiuta le organizzazioni a valutare la propria resilienza contro gli attacchi DDoS. Gli attacchi DDoS possono interrompere i servizi sovraccaricando i sistemi ICT con una marea di traffico, rendendoli inaccessibili agli utenti legittimi. La piattaforma di test DDoS automatizzata di Mazebolt simula attacchi DDoS reali per valutare la capacità di un'organizzazione di resistere a tali minacce, aiutandola a identificare i punti deboli e a implementare misure di mitigazione efficaci.

Oltre a TIBER e ai tool di test automatizzati come Mazebolt, le organizzazioni possono avvalersi di altri servizi e strumenti di valutazione di terze parti per garantire la conformità ai requisiti del DORA. Questi possono includere strumenti di scansione delle vulnerabilità, servizi di

penetration test e framework di audit della sicurezza, tutti finalizzati a identificare e affrontare i rischi per la sicurezza e a migliorare la resilienza operativa.

Regulatory Technical Standards (RTS) DORA.

Analizziamo più a fondo gli RTS (Regulatory Technical Standards) associati al Digital Operational Resilience Act (DORA) e le loro implicazioni per le imprese e le istituzioni finanziarie.



Gli RTS sviluppati nell'ambito del DORA forniscono specifiche tecniche dettagliate e linee guida per implementare efficacemente i requisiti della legge. Essi rappresentano un framework di riferimento da seguire per le organizzazioni, assicurando coerenza e uniformità nei loro sforzi per migliorare la resilienza operativa e la cybersecurity.

Gli elementi chiave degli RTS DORA includono:

Governance e Gestione del Rischio: L'RTS delinea i requisiti per la definizione di solidi framework di governance e gestione del rischio per verificare la resilienza operativa e gli sforzi di cybersecurity. Ciò include la definizione di ruoli e responsabilità, la conduzione di valutazioni del rischio e la definizione di politiche e procedure per mitigare efficacemente i rischi identificati.

Gestione degli Incidenti e Reporting: Vengono fornite linee guida dettagliate per la segnalazione e la gestione degli incidenti, specificando i tipi di incidenti che devono essere segnalati, i tempi di segnalazione e le informazioni che devono essere incluse nei rapporti sugli incidenti. Questo facilita una risposta rapida ed efficace agli incidenti informatici, riducendo al minimo il loro impatto sulle operazioni.

Risk Management di Terze Parti: L'RTS sottolinea l'importanza della gestione del rischio di terzi parti, richiedendo alle organizzazioni di valutare e monitorare le pratiche di sicurezza dei loro fornitori di servizi e fornitori terzi. Ciò include la conduzione di valutazioni di due diligence, l'implementazione di disposizioni contrattuali e l'istituzione di meccanismi di supervisione e valutazione continua.

Misure di Security ICT: Vengono delineate misure e controlli di sicurezza specifici per la protezione dalle minacce informatiche, come l'accesso non autorizzato, la violazione dei dati e le infezioni da malware. Ciò include misure relative al controllo degli accessi, alla crittografia, alla sicurezza della rete e al monitoraggio della sicurezza, adattate al profilo di rischio e ai requisiti operativi dell'organizzazione.

Esercizi e Test di Resilienza: L'RTS fornisce indicazioni sulla conduzione di test ed esercitazioni di resilienza per valutare l'efficacia delle misure di resilienza operativa. Ciò include requisiti per simulazioni basate su scenari, esercitazioni di red teaming e verifiche post-incidente per identificare i punti deboli e le possibili opportunità di miglioramento.

L'implementazione degli RTS sviluppati nell'ambito del regolamento DORA richiede uno sforzo coordinato tra i vari settori dell'organizzazione, tra cui l'IT, la gestione del rischio, la compliance e l'alta dirigenza. Si tratta di allineare i processi e i controlli esistenti ai requisiti delineati negli RTS, nonché di implementare nuove misure, ove necessario, per garantire la conformità.

Inoltre, la conformità agli RTS è soggetta alla supervisione e all'applicazione della normativa, con le autorità competenti responsabili del controllo della conformità e dell'applicazione di sanzioni in caso di non conformità. Ciò sottolinea l'importanza di adottare le misure necessarie per soddisfare i requisiti delineati negli RTS e dimostrare l'impegno verso la resilienza operativa e la cybersecurity.

Nel complesso, gli RTS DORA forniscono alle organizzazioni una chiara roadmap per migliorare la resilienza operativa e la sicurezza informatica nel

settore finanziario. Seguendo le linee guida delineate negli RTS, le imprese e le istituzioni finanziarie possono rafforzare le loro difese contro le minacce informatiche e le interruzioni operative, salvaguardando in ultima analisi la stabilità e l'integrità del sistema finanziario.

Requisiti Uniformi per la Resilienza Operativa Digitale: Comprendere DORA e gli RTS (Regulatory Technical Standards)

Il Digital Operational Resilience Act (DORA) segna un passo fondamentale per rafforzare la sicurezza delle reti e dei sistemi informativi delle imprese e organizzazioni del settore finanziario. DORA prevede un quadro normativo unificato volto a garantire la resilienza operativa digitale, obbligando tutte le società finanziarie a rafforzare la loro capacità di resistere, rispondere e riprendersi da varie interruzioni e minacce legate all'ICT. Con la sua attuazione, l'Unione Europea (UE) si sforza di promuovere un ambiente sicuro, prevenendo e mitigando le minacce informatiche in modo coerente in tutti gli Stati membri.

Alle Autorità Europee di Vigilanza (ESA), in collaborazione con l'Agenzia dell'Unione Europea per la Cybersecurity (ENISA), è stato conferito il mandato di sviluppare le Norme Tecniche di Regolamentazione (RTS), ai sensi degli articoli 15 e 16 del DORA. Sulla base degli standard europei e internazionali esistenti in materia di gestione del rischio ICT, come le linee guida dell'EBA, la direttiva NIS2 e gli standard ISO, le ESA mirano a sviluppare RTS completi per integrare le disposizioni contenute nel DORA.

In particolare, i mandati comprendono aspetti specifici della gestione del rischio ICT, tra cui la governance, la protezione, il rilevamento, la risposta e il ripristino. Questi RTS sono destinati a lavorare in sinergia con il regolamento DORA, rafforzando la resilienza complessiva delle entità finanziarie contro le minacce informatiche e le interruzioni operative.

L'architettura della bozza degli RTS proposta riflette una meticolosa integrazione con i quadri europei e internazionali esistenti in materia di ICT e information security. La bozza degli RTS mantiene la neutralità tecnologica, evitando di approvare prodotti o tecnologie specifiche per garantire la sicurezza del futuro. Inoltre, gli RTS si sforzano di essere intersettoriale e indipendente dal settore, incorporando principi applicabili a tutte le entità che rientrano nell'ambito di applicazione del DORA, pur accogliendo, ove necessario, requisiti specifici per le entità.

In sostanza, gli RTS in ambito del Regolamento DORA fungono da pietra miliare per la costituzione di solidi framework di gestione del rischio ICT nelle entità finanziarie. Aderendo a questi standard, le organizzazioni possono rafforzare la loro postura di cybersecurity e garantire un'ininterrotta continuità operativa di fronte all'evoluzione delle minacce. Con il progredire del DORA e dei relativi RTS, è indispensabile che le entità finanziarie conformino le proprie politiche e pratiche a questi sviluppi normativi, rafforzando così la resilienza digitale del settore finanziario europeo.

Conclusioni: Rafforzare la Resilienza del Settore Finanziario

L'introduzione del Digital Operational Resilience Act (DORA) rappresenta un momento decisivo per la difesa contro le minacce informatiche e le interruzioni operative nel settore finanziario. Introducendo un quadro normativo unificato, DORA mira a rafforzare la sicurezza delle reti e dei sistemi informativi delle entità finanziarie che operano all'interno dell'Unione Europea (UE), introducendo una nuova era di resilienza digitale.

L'approccio proattivo del DORA ai test di resilienza digitale, caratterizzato dall'incentivazione all'ethical hacking e al penetration test, segna un significativo allontanamento dai paradigmi normativi tradizionali. Questo cambiamento sottolinea l'importanza di adottare una mentalità "breaking bad", in cui le organizzazioni testano attivamente le proprie difese per identificare le vulnerabilità e rafforzare in modo preventivo la propria postura di cybersecurity.

I pillar fondamentali del DORA, tra cui la segnalazione e la gestione degli incidenti, la gestione del rischio ICT di terzi, la resilienza operativa, le misure di sicurezza e gli accordi di governance generale, pongono le basi per un solido framework di cybersecurity nel settore finanziario. La conformità a questi pillar non è solo un requisito normativo, ma un imperativo strategico per le organizzazioni che cercano di salvaguardare le proprie operazioni e la propria reputazione in un mondo sempre più digitalizzato.

Il framework Threat Intelligence-Based Ethical Red Teaming for the European Union (TIBER-EU) si rivela uno strumento fondamentale per il raggiungimento degli obiettivi del DORA, in particolare per i test di resilienza informatica. Simulando scenari di attacco e di minacce informatiche reali, TIBER-EU consente alle organizzazioni di identificare le vulnerabilità, testare la propria resilienza e rafforzare le difese contro le minacce informatiche.

Anche l'automazione svolge un ruolo cruciale nel migliorare la resilienza operativa e l'efficacia della sicurezza informatica. I tool automatizzati, come le piattaforme di test DDoS, semplificano le attività di routine, migliorano i tempi di risposta e facilitano il monitoraggio e la valutazione continui dei sistemi ICT, migliorando così la capacità di un'organizzazione di rilevare e mitigare efficacemente le minacce informatiche.

Insieme a TIBER-EU e ai tool di test automatizzati, gli Regulatory Technical Standards (RTS) DORA forniscono alle organizzazioni una chiara tabella di marcia per migliorare la resilienza operativa e la cybersecurity nel settore finanziario. Aderendo a questi standard e avvalendosi di servizi e strumenti di valutazione di terze parti, le organizzazioni possono affrontare le complessità del DORA con fiducia, sapendo di essere preparate a fronteggiare un panorama di minacce in continua evoluzione.

In sintesi, il regolamento DORA rappresenta un fondamentale passo avanti verso la promozione della resilienza digitale e la salvaguardia della stabilità e dell'integrità del sistema finanziario. Aderendo ai principi dell'ethical hacking, sfruttando strumenti e framework innovativi e rispettando gli standard normativi, le organizzazioni possono muoversi nel panorama delle minacce in continua evoluzione con resilienza e fiducia, garantendo la continuità della fiducia e della sicurezza dei servizi finanziari nell'era digitale. ■

La Direttiva NIS2: un'opportunità per elevare il livello di cyber security del Paese.

Autore: Rossella Macinante,
BU Leader NetConsulting cube

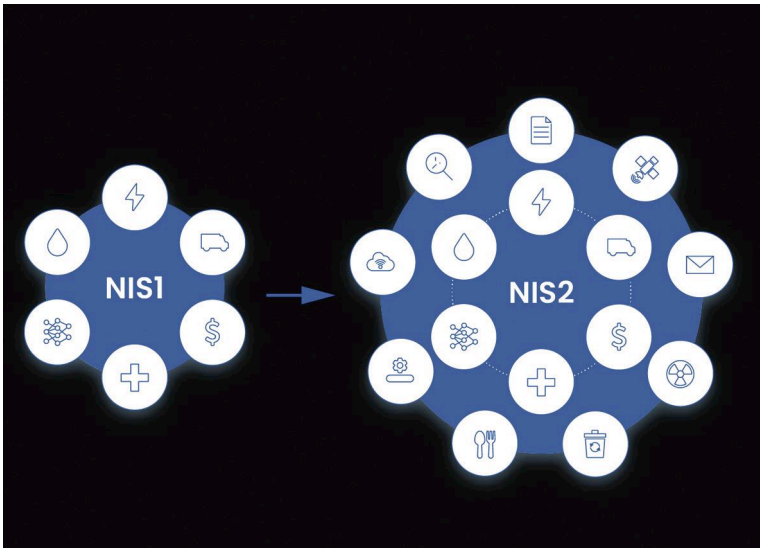
L'evoluzione degli attacchi cyber e le conseguenze in termini di sospensione di servizi, in alcuni casi anche essenziali, insieme alla digitalizzazione, ormai capillare ed estesa in tutti i settori, hanno reso necessario una revisione del quadro normativo europeo sul tema della cyber sicurezza.

La NIS2, il cui testo definitivo è stato approvato a dicembre 2022, dovrà essere adottata e pubblicata dai paesi dell'Unione entro il 17 ottobre 2024, con conseguente abrogazione della normativa precedentemente in vigore ovvero la NIS1. L'obiettivo principale che ha guidato il legislatore è stato quello di rendere uniforme l'applicazione della normativa nei paesi dell'Unione Europea, estendendone il perimetro e rendendo gli adempimenti più stringenti, per sopperirne alcune carenze nell'attuazione che rischiavano di creare difformità in termini di resilienza e capacità di difesa tra i paesi europei. Inoltre, sempre al fine di migliorare la postura di sicurezza, la NIS2 introduce nuovi obblighi, tra cui ad esempio la nomina di una figura con competenze e responsabilità in ambito cyber security per le

organizzazioni soggette alla normativa, sia più ampi poteri alle autorità di vigilanza che potranno intervenire con ispezioni in ottica preventiva, oltre che ex post.

La volontà del legislatore è innalzare la postura di sicurezza della maggior parte delle organizzazioni, per contrastare tempestivamente la velocità con cui si può propagare l'attacco grazie all'interconnessione dei sistemi tra soggetti diversi.

Una delle principali carenze della NIS1 riguardava il numero limitato di settori a cui era rivolta e l'arbitrarietà con cui i diversi Stati potevano definire il cosiddetto perimetro di sicurezza cibernetica. Questo limite è stato superato ridefinendo ed estendendo l'ambito di applicazione e le categorie di settori, prima circoscritte all'interno della denominazione di operatori di servizi essenziali e operatori digitali. Per ovviare a questo, la NIS2 prevede un elenco puntuale di settori, che senza dubbio risulta più ampio rispetto a quello definito dalla NIS1 includendo accanto ai settori essenziali dell'energia, dei trasporti, delle banche, delle infrastrutture finanziarie, dell'acqua, della sanità e delle infrastrutture digitali, anche fornitori di servizi digitali nei settori dell'e-commerce, motori di ricerca, cloud computing, gestione dei servizi ICT. Una delle novità più significative è l'inclusione nell'elenco degli altri "settori critici" in cui rientrano numerose categorie merceologiche quali i servizi postali, gestione dei rifiuti, produzione e distribuzione di sostanze chimiche, produzione di alimenti, fabbricazione di dispositivi medici, fabbricazione di computer ed elettronica, fabbricazione di apparecchiature elettriche, fabbricazione di macchinari, fabbricazione di autoveicoli, fornitori di servizi digitali, organizzazioni di ricerca.



Un ulteriore elemento di novità è poi rappresentato dal riferimento alla dimensione dell'operatore, includendo nel perimetro non solo le grandi organizzazioni, ma anche quelle denominate "medie" in cui rientrano le imprese che occupano meno di 250 persone, il cui fatturato annuo non supera i 50 milioni di euro oppure il cui totale di bilancio annuo non supera i 43 milioni di euro". Ci sono poi delle ulteriori caratteristiche, in presenza delle quali, l'ente o l'impresa indipendentemente dalla dimensione, è soggetto agli obblighi previsti da NIS2. Sono quindi considerati nella definizione del perimetro l'esclusività nell'erogazione del servizio (in caso il soggetto sia unico fornitore di un servizio considerato essenziale), l'impatto che avrebbe a livello di sicurezza nazionale, di salute pubblica o comunque a livello di sistema Paese un'interruzione o una perturbazione del servizio erogato, in particolare se si potrebbe avere un impatto transfrontaliero.

Infine, da considerare come un importante passo avanti rispetto alla NIS1 l'inclusione degli enti che rientrano nella Pubblica Amministrazione centrale e regionale, con riferimento, per questi ultimi, ad enti che erogano servizi la cui interruzione rappresenti un rischio per l'economia o per la sicurezza. Viene lasciata discrezione ai singoli stati relativamente all'inclusione di enti della pubblica amministrazione locale o agli istituti di istruzione.

Entro il 17 aprile 2025, gli stati dell'Unione dovranno presentare un elenco dei soggetti essenziali e importanti, nonché dei soggetti che forniscono servizi di registrazione di dominio (anch'essi inclusi nella normativa). L'elenco dovrà essere rivisto e presentato per il riesame almeno ogni due anni.

Le misure che le organizzazioni a cui si applica la norma dovranno adottare sono sia di tipo organizzativo che di tipo tecnico e vanno da un coinvolgimento nella governance aziendale nella gestione rischi della cybersicurezza all'adozione di un approccio multirischio, all'obbligo di notifica di eventuali incidenti significativi entro tempistiche definite (seppure con un approccio graduale).

Inoltre, sul fronte dei prodotti e servizi IT da adottare viene rilasciato ai singoli stati membri facoltà di decidere se imporre un percorso di certificazione nell'ambito dei sistemi europei di certificazione della cybersicurezza,

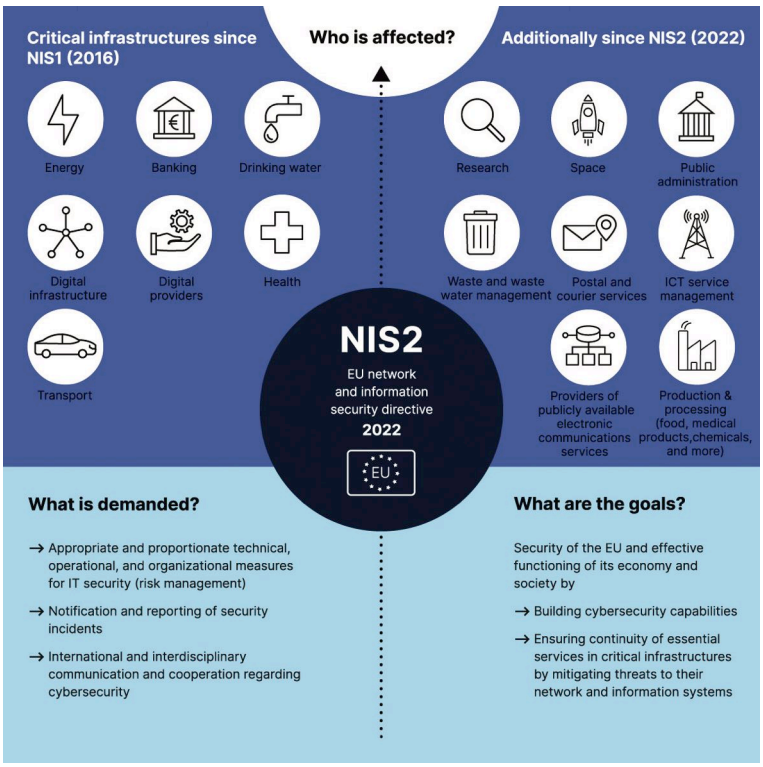
BIO

Rossella Macinante è BU leader in NetConsulting cube degli ambiti Cybersecurity, Government e Finance, con un'esperienza consolidata nell'analisi delle evoluzioni tecnologiche che abilitano i processi di digitalizzazione delle imprese e, in particolare, sui trend della Cybersecurity presso le aziende italiane e sull'andamento dei suoi principali attori. Da 5 anni è responsabile del progetto Barometro Cybersecurity 4.0, che si struttura in una serie di incontri nel corso dell'anno su temi di rilevanza in ambito cybersecurity su cui si confrontano aziende della domanda e dell'offerta. Il Barometro, inoltre, si basa su una survey finalizzata a fornire un quadro esaustivo, costantemente aggiornato e completo sul livello di maturità in ambito Cybersecurity delle principali aziende e organizzazioni italiane.

strada che per esempio nel caso della PA italiana è stata già intrapresa con i cosiddetti CSIRT.

Il tema che avrà maggior impatto, analizzando la norma nel dettaglio, è quello relativo all'adozione di misure tecniche e organizzative che dovranno essere commisurate al rischio. Tali misure dovranno comprendere non solo l'analisi dei rischi e di sicurezza dei sistemi informatici, ma anche la gestione degli incidenti con tecnologie adeguate e politiche che assicurino la business continuity. Sul fronte delle misure organizzative la formazione in materia di cybersecurity rappresenta un aspetto fondamentale e dovrà essere rivolta non solo ai dipendenti ma anche ai membri del board. Più in generale, le misure previste dalla NIS2 comprendono tutte le tecniche di difesa e di governance della cybersecurity per innalzare le barriere e garantire una maggiore resilienza del sistema economico e produttivo europeo. La norma non si limita a definire obblighi per i soggetti "essenziali" ed "importanti", ma si estende anche alla catena di approvvigionamento che dovrà essere messa in sicurezza.

Il riferimento alla Supply Chain fa comprendere l'ampia portata della nuova NIS2 e l'impatto che avrà non solo sulle aziende che fanno riferimento ai settori essenziali o importanti, definiti nella norma, ma anche su aziende che fanno parte di un ecosistema più ampio, in quanto potenzialmente dovranno a loro volta interfacciarsi con i soggetti essenziali e importanti lungo la catena del valore. In conclusione, NIS2 richiederà investimenti crescenti per molte aziende che ancora non presentano misure o tecniche adeguate sul fronte cybersecurity. Dalle stime di NetConsulting cube il mercato della Cybersecurity in Italia supererà i 2, 4 miliardi di euro già alla fine del 2024 e proseguirà a crescere a tassi superiori



al 12% nei prossimi anni, supportato anche dal processo di trasformazione digitale della PA e della Sanità.

L'adozione di servizi SOC, di soluzioni di Multifactor Authentication, di crittografia o strumenti per la governance end-to-end della sicurezza di sistemi e applicazioni rappresenteranno ambiti di investimento prioritari. Tra i settori storicamente più arretrati, Sanità, Pubblica amministrazione e Retail sono quelli che dovranno maggiormente impegnarsi per colmare il gap più elevato. Un ulteriore ambito evolutivo riguarderà la messa in sicurezza degli ambienti OT, che soprattutto negli operatori di settori definiti "essenziali" come Energy e Utilities, Trasporti e reti idriche, estendo anche ai produttori di reti ed impianti obblighi di certificazione. ■

NIS, NIS2, Golden Power e perimetro di Sicurezza Cibernetica Nazionale.

Autore: Corradino Corradi

Il quadro normativo di cybersecurity europeo e italiano è particolarmente articolato e negli anni si è stratificato con interventi normativi non armonizzati tra loro.

Nell'articolo sono riportati i più recenti provvedimenti europei e italiani, con un focus specifico sul settore delle telecomunicazioni italiane.

Regolamento n. 881/2019 (Cybersecurity Act)

Il Regolamento n. 881/2019 (Cybersecurity Act) ha introdotto due novità principali nel panorama della cybersecurity europea:

- la creazione di un quadro permanente per la cooperazione tra le autorità nazionali competenti in materia di cybersecurity, coordinato **dall'Agenzia dell'Unione europea per la cybersecurity (ENISA)**;
- l'istituzione di un sistema di certificazione europeo per i prodotti, i servizi e i processi di cybersecurity, volto a garantire un livello elevato e uniforme di sicurezza in tutta l'Unione. Il Regolamento è entrato in vigore il 27 giugno 2019 ed è direttamente applicabile in tutti gli Stati membri.

L'ENISA ha il compito di contribuire a migliorare la capacità e la resilienza della rete e dei sistemi informativi nell'UE, nonché a promuovere la cooperazione e lo scambio di informazioni tra gli Stati membri e le istituzioni dell'UE. L'ENISA è stata creata nel 2004 con il regolamento (CE) n. 460/2004 e ha sede ad Atene, in Grecia, con un ufficio secondario a Heraklion, in Creta. In ottemperanza al Cybersecurity Act, l'ENISA svolge inoltre un ruolo di supporto nella definizione e nell'attuazione delle politiche e delle normative in materia di cybersecurity a livello europeo.

Direttiva n. 2557/2022 sulla resilienza dei soggetti critici (Direttiva CER – Resilience of Critical Entities)

La Direttiva CER sulla resilienza dei soggetti critici (Direttiva CER) è una normativa dell'Unione europea che mira a rafforzare la sicurezza e la resilienza delle entità che forniscono servizi essenziali in settori strategici come quello di energia, trasporti, finanziario, sanità, alimentare e acqua.

La direttiva europea stabilisce requisiti minimi di sicurezza per le entità critiche e prevede una maggiore cooperazione tra gli Stati membri e la Commissione europea nella gestione dei rischi e degli incidenti transfrontalieri.

La direttiva sostituisce e amplia la precedente Direttiva 2008/114/CE sui soggetti critici per le infrastrutture europee (EPCIP), introducendo:

- nuovi obblighi di notifica degli incidenti di sicurezza;
- necessità di condurre audit periodici;
- creazione di piani di sicurezza;
- necessità di effettuare periodici test di resistenza.

La direttiva è stata adottata dal Parlamento europeo e dal Consiglio il 14 dicembre 2022 ed è entrata in vigore il 16 gennaio 2023. Gli Stati membri hanno tempo fino al 17 ottobre 2024, per recepire la direttiva nel diritto nazionale.

Direttiva NIS 2 (Dir. n. 2555/2022)

La Direttiva NIS 2 sulla sicurezza delle reti e dei sistemi informativi è una normativa dell'Unione europea che mira a rafforzare la capacità di prevenire, affrontare e rispondere agli incidenti informatici che possono avere un impatto significativo sul mercato interno e sulla società.

La direttiva aggiorna e sostituisce la precedente Direttiva NIS del 2016 (NIS1). I cinque punti salienti della direttiva NIS 2 sono:

- la definizione di incidente informatico come qualsiasi evento che ha un effetto negativo sulla sicurezza delle reti e dei sistemi informativi, indipendentemente dalla sua origine, natura, durata o impatto;
- l'introduzione di una scala comune per valutare la gravità degli incidenti informatici, basata su cinque criteri: numero di utenti colpiti, durata dell'interruzione, aree geografiche interessate, grado di degrado del servizio e impatto trasversale;
- l'obbligo per gli OSE e i FSD di notificare gli incidenti informatici alle autorità nazionali competenti entro 24 ore dalla loro conoscenza o presunzione, e di fornire informazioni dettagliate entro 72 ore;
- l'istituzione di un regime sanzionatorio uniforme per gli OSE e i FSD che non rispettano i requisiti della direttiva, che può prevedere multe fino al 2% del fatturato annuo globale o a 10 milioni di euro, a seconda di quale sia il maggiore;
- il rafforzamento del ruolo dell'ENISA, che diventa l'autorità di riferimento per la sicurezza informatica nell'UE, con il compito di assistere gli Stati membri e la Commissione nella definizione e nell'attuazione delle politiche e delle misure in materia di NIS.

Tra le novità introdotte dalla Direttiva NIS2, rispetto a NIS1, vi sono:

- l'ampliamento dell'ambito di applicazione della direttiva a nuovi settori strategici per l'economia e la società digitale, quali il cloud computing, i social network, i fornitori di servizi di pagamento online, i servizi di identificazione elettronica, nonché le infrastrutture critiche per la salute, l'energia, il trasporto, la gestione delle acque e dei rifiuti;
- l'introduzione di un quadro armonizzato di requisiti minimi di sicurezza informatica per gli operatori di servizi essenziali (OSE) e i fornitori di servizi digitali (FSD), basato su principi generali e standard internazionali, che devono essere adeguati al livello di rischio e al profilo di maturità degli operatori;
- la previsione di una maggiore cooperazione tra gli Stati membri, attraverso lo scambio di informazioni, la realizzazione di esercitazioni congiunte, la creazione di gruppi di lavoro tematici e la designazione di punti di contatto nazionali per la NIS.

La Direttiva NIS2 dovrà essere recepita dagli Stati membri entro il 17 ottobre 2024. In Italia, il processo di attuazione della normativa europea in materia di sicurezza informatica è ancora in fase preliminare. Al momento, c'è una proposta di legge di recepimento e sono in atto le consultazioni con tutti i soggetti pubblici e privanti interessati ed impattati dalla normativa.

Reg. n. 2554/2022 (DORA)

Il DORA (Digital Operational Resilience Act) è un regolamento europeo che mira a rafforzare la resilienza operativa delle entità del settore finanziario nell'affrontare i rischi informatici.

Il regolamento DORA si applica a un'ampia gamma di entità, tra cui banche, assicurazioni, fondi pensione, società finanziarie, operatori di sistemi di pagamento e cripto-asset service provider. La normativa prevede una serie di requisiti per le entità finanziate, tra cui: la gestione dei rischi informatici, la valutazione della conformità dei fornitori di servizi ICT, il testing delle infrastrutture critiche, l'incident reporting e il monitoraggio della supervisione.

DORA introduce anche un meccanismo di "oversight" per gli operatori di servizi ICT critici, che forniscono soluzioni tecnologiche essenziali per le entità finanziate, come il cloud computing, i big data o l'intelligenza artificiale. Questi operatori dovrebbero ottenere una certificazione dell'UE e sottostare al controllo delle autorità competenti.

Il DORA è direttamente applicabile in tutti gli Stati membri dell'UE, senza bisogno di recepimento nelle legislazioni nazionali. Tuttavia, gli Stati membri dovranno adeguare le proprie normative e autorità di vigilanza ai requisiti e alle competenze previste dal DORA.

BIO

Corradino Corradi è responsabile della funzione ICT Security & Fraud Management di Vodafone Italia e all'interno del Gruppo Vodafone nel mondo ricopre il ruolo di Senior Member del Corporate Security Leadership Team. L'Ing. Corradi ha 10 anni di esperienza nel campo della security e della gestione delle frodi, della sicurezza dei pagamenti e della protezione delle infrastrutture critiche; è responsabile dell'implementazione delle strategie di sicurezza proattive e reattive, del coordinamento delle operazioni antifrode, nonché del coordinamento di grandi team di professionisti della sicurezza. Corradino Corradi è anche responsabile della gestione dei piani di Business Continuity e Crisis Management di Vodafone Italia. Ha inoltre esperienza nei settori di Risk Management, Compliance, Privacy e Data Protection, Awareness & Training di Frodi e Security, Security Operations Center e CERT, Security Audit e Certificazioni (ISO 27001, SOX, BS25999). In precedenza ha maturato più di 5 anni di esperienza come IT & Security Manager per i principali operatori italiani di telecomunicazioni e banche internazionali.

Perimetro di Sicurezza Nazionale Cibernetica (PSNC)

Il Perimetro di Sicurezza Nazionale Cibernetica (PSNC) è un sistema di protezione delle infrastrutture critiche nazionali, che comprende le reti e i sistemi informativi pubblici e privati essenziali per la sicurezza, la difesa, l'ordine pubblico, la salute, l'energia, le comunicazioni e il funzionamento dei servizi finanziari. Il PSNC è stato

istituito il 21 settembre 2019, con il decreto-legge n. 105/2019, convertito con la legge n. 133/2019.

Il PSNC prevede l'identificazione degli operatori di tali infrastrutture, che devono rispettare specifici obblighi in materia di sicurezza informatica, tra cui l'adozione di misure organizzative, tecniche e procedurali, la notifica di eventuali incidenti, la partecipazione a esercitazioni e test, la cooperazione con le autorità competenti e il rispetto di vincoli di localizzazione dei dati e delle attività.

Il PSNC stabilisce anche le modalità di intervento del Governo in caso di crisi cibernetica; in particolare Il PSNC attribuisce al Presidente del Consiglio dei Ministri il potere di adottare misure di salvaguardia, anche eccezionali e urgenti, nei confronti degli operatori del PSNC, qualora sussistano gravi e imminenti minacce alla sicurezza nazionale. Il PSNC prevede infine sanzioni amministrative e penali per gli operatori che violano gli obblighi previsti dalla normativa.

Un ruolo chiave nella attuazione del PSNC è dato alla **Agenzia Nazionale per la Cybersecurity (ACN)**. ACN è un ente pubblico dotato di autonomia organizzativa e finanziaria, istituito con il decreto Legge n.82 del 14 giugno 2021, convertito con la legge del 4 agosto 2021, n. 109.

La missione di ACN è quella di garantire la sicurezza cibernetica del Paese, attraverso la prevenzione, il contrasto e la gestione delle minacce informatiche che possono compromettere le infrastrutture critiche nazionali, le attività strategiche e gli interessi vitali della Nazione. Il suo ruolo per l'attuazione del Perimetro di Sicurezza Nazionale Cibernetica (PSNC) è quello di:

- definire i criteri e le modalità per l'individuazione degli operatori del PSNC e dei soggetti equiparati;
- svolgere funzioni di supervisione, controllo e supporto tecnico-operativo sugli operatori del PSNC e sui soggetti equiparati;
- collaborare con il Dipartimento delle Informazioni per la Sicurezza (DIS) e con il Comitato Interministeriale per la Sicurezza della Repubblica (CISR) per la valutazione delle minacce e dei rischi cibernetici;
- predisporre piani ed esercitazioni per la gestione delle crisi cibernetiche, in coordinamento con il Dipartimento della Protezione Civile;
- partecipare alle attività di cooperazione internazionale in materia di sicurezza cibernetica, in rappresentanza dell'Italia.

La disciplina Golden Power, che trova origine e fondamento nel decreto-legge 15 marzo 2012, n. 21, (convertito con modificazioni dalla legge n. 56 dell'11 maggio 2012), ha impatto significativo negli assetti societari, nella governance aziendale e nelle operazioni di M&A extra-transazionali. Alcuni aspetti della normativa riguardano anche la cyber-sicurezza.

La Golden Power negli anni ha subito numerosissime modifiche e integrazioni. La più significativa in ambito telecomunicazioni è il D.L. n. 21 del 2012, **l'articolo 1-*bis***, che disciplina **l'esercizio dei poteri speciali inerenti le reti di telecomunicazione elettronica a banda larga con tecnologia 5G**.

L'articolo stabilisce che il Governo ha poteri speciali sulle reti di telecomunicazione elettronica a banda larga con tecnologia 5G, quando queste sono rilevanti per la sicurezza nazionale o la difesa. I poteri speciali consistono in:

- l'obbligo di comunicare al Governo ogni operazione di acquisizione o alienazione di partecipazioni, beni o rapporti giuridici riguardanti le reti 5G;
- l'autorizzazione preventiva del Governo per qualsiasi accordo o contratto con fornitori di componenti o servizi per le reti 5G, se questi provengono da paesi terzi all'Unione europea o all'area economica europea;
- la possibilità di imporre prescrizioni o divieti alle imprese che gestiscono le reti 5G, per garantire la sicurezza e il funzionamento delle stesse.
- misure di sicurezza ad-hoc per l'accesso da remoto dei fornitori degli apparati di telecomunicazioni (vedi MFA e tracciamento delle operazioni), la review e il test periodico del codice (come DAST e SAST), dettagliate procedure di configuration and release management.

Termino la carrellata di normative di cyber-security citando anche direttive europee che coprono ambiti continui alla cyber-security ma che hanno un impatto sulla sicurezza informatica sia a livello strategico che operativo; su tutte il **GDPR** per privacy e data protection e **l'EU Artificial Intelligence Act** per quel che riguarda l'uso consapevole e sicuro dell'AI.

Il PSNC, la disciplina Golden Power e le altre normative nazionali in materia di sicurezza informatica e resilienza operativa dovranno necessariamente essere coordinati e armonizzati con la NIS 2 (per tutte le infrastrutture critiche) e il DORA (per il settore finanziario), al fine di evitare sovrapposizioni o conflitti tra i diversi livelli di regolazione e supervisione.

La necessità di contrastare il "cybercrime" e gli "state sponsored attack" richiede focalizzazione da parte delle infrastrutture critiche italiane (in gran parte private) e un approccio che sia "risk-based" e non meramente finalizzato alla mera compliance normativa. È fondamentale quindi incoraggiare qualsiasi azione volta a semplificare il quadro normativo e di compliance alla cyber-security e facilitare la collaborazione tra pubblico (in particolare con ACN) e privato. ■

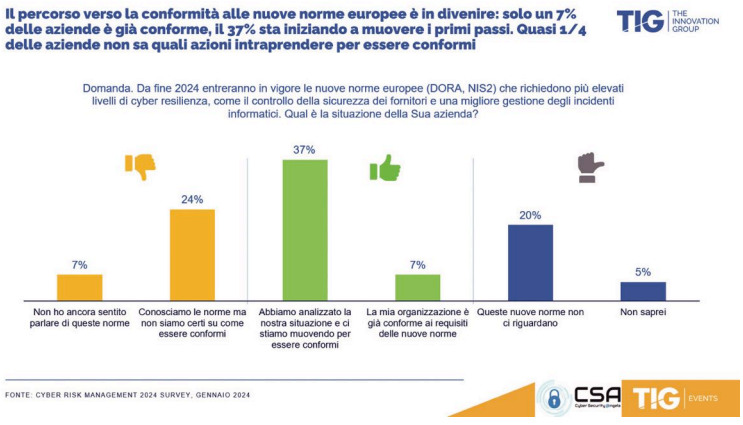
Compliance europea alle porte per la resilienza delle imprese italiane.

Autore: **Elena Vaciago**

L'imminente entrata in vigore di importanti normative europee sta ponendo nuove sfide e responsabilità alle aziende, in particolare ai vertici aziendali e ai membri del Board. Il regolamento DORA nel mondo finanziario, la direttiva NIS 2 nei settori critici o importanti per gli Stati, introducono requisiti rigorosi per garantire l'operatività e la sicurezza digitale delle aziende, con sanzioni severe per chi non rispetta tali disposizioni.

Ad esempio, la mancata conformità alla direttiva NIS 2, oltre a sanzioni importanti in caso di inadempienza (fino a 10 milioni di euro o il 2% del fatturato mondiale annuo nel caso di servizi essenziali) potrebbe comportare la sospensione delle autorizzazioni e delle concessioni, con la possibilità di sospendere il CEO dal suo ruolo. Inoltre, il bacino delle industrie coinvolte nella direttiva è notevolmente ampliato rispetto alla precedente NIS, includendo settori come l'industria, l'agroalimentare, il chimico e il farmaceutico, che hanno in Italia una grande rilevanza economica.

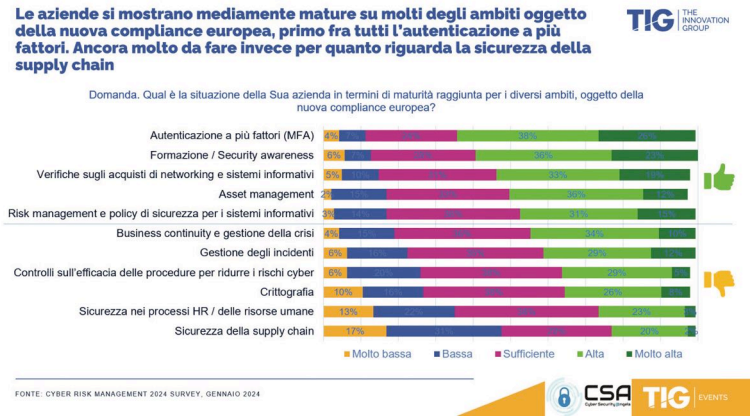
Tuttavia, nonostante l'imminenza di queste normative, molte aziende sembrano ancora non essere pronte per la conformità. The Innovation Group svolge annualmente, insieme alla community di CISO Cyber Security Angels, una survey per verificare i percorsi delle aziende italiane in ambito Cyber risk management. Nel gennaio 2024, intervistando un campione di 166 aziende medio grandi in merito alla preparazione alle nuove norme europee, è emerso che solo una percentuale molto ridotta delle aziende (circa il 7%) si considerava già conforme alle nuove norme. La maggioranza, il 37%, ha affermato che stava iniziando solo ora a muovere i primi passi verso la conformità.



[figura - Capitolo Cyber - IMG0]

Entrando più nel dettaglio, andando quindi a indagare la maturità sui diversi ambiti della compliance europea, si osserva che la situazione è in media sufficiente per quanto riguarda l'adozione di misure e strumenti come: Autenticazione a più fattori (MFA); formazione / Security awareness; verifiche sugli acquisti di networking e sistemi informativi; asset management; risk management e policy di sicurezza per i sistemi informativi. Dove invece c'è ancora molta strada da fare è per tutto quanto riguarda la gestione degli incidenti, i controlli per garantire che le misure e i processi in essere siano efficaci, la sicurezza della supply chain. Quest'ultimo aspetto in particolare, la verifica della sicurezza di fornitori e terze parti, risulta essere un ambito particolarmente critico, che richiederebbe attenzione e investimenti

adeguati a garantire la protezione dei dati e delle operazioni aziendali.



[figura - Capitolo Cyber – IMG2]

A dimostrazione quindi del fatto che il percorso verso la conformità alle nuove normative europee è in corso, e molte aziende dovranno nei prossimi mesi accelerare i propri sforzi per adeguarsi ai requisiti imposti. È essenziale che le aziende italiane prendano sul serio queste disposizioni e adottino misure concrete per garantire la sicurezza e l'operatività delle proprie infrastrutture digitali, al fine di evitare sanzioni e proteggere la reputazione e l'operatività.

La cybersecurity come elemento abilitante la Trasformazione Digitale

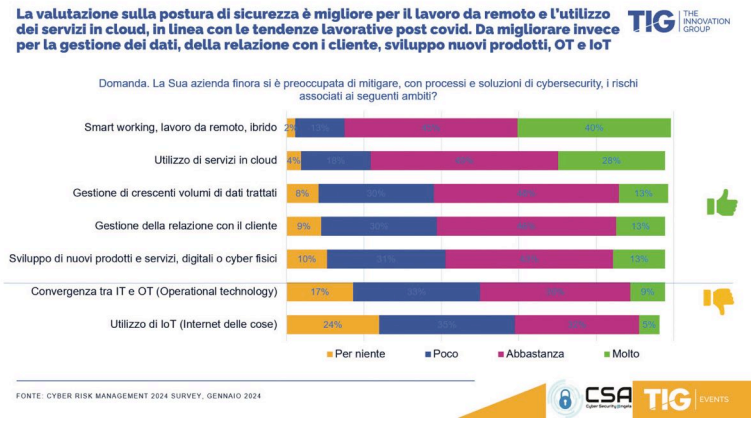
La cybersecurity è diventata una componente indispensabile nel determinare il successo delle iniziative di Trasformazione Digitale, e le aziende stanno riconoscendo l'importanza di investire nelle risorse e nelle competenze necessarie per garantire una protezione efficace contro le minacce informatiche in continua evoluzione.

È incoraggiante notare che gli investimenti in soluzioni e servizi per la cybersecurity stanno crescendo costantemente. Dall'indagine di The Innovation Group e Cyber Security Angels emerge che la spesa media nel 2023 è stata dell'8,3% rispetto al budget ICT complessivo, con una previsione di crescita fino al 9% entro il 2024. È interessante notare che le voci di spesa che registreranno il maggiore incremento includono gli acquisti di soluzioni tecnologiche di cybersecurity; la preparazione agli incidenti; la formazione e l'acquisto di servizi di consulenza in materia di cybersecurity, nonché la spesa per il personale interno e per i Security Operation Center (SOC).

Si osserva inoltre nelle aziende italiane un crescente ricorso a terzi, come società specializzate, system integrator e vendor di cybersecurity, per affrontare i complessi aspetti del piano di cyber risk management. Alcuni ambiti, poi, sono oggi completamente esternalizzati in molte realtà aziendali, a conferma della necessità di expertise specializzate e risorse dedicate per affrontare queste sfide.

Il programma di Cyber Risk Management continua a evolvere

La consapevolezza dell'importanza della cybersecurity nell'era della Trasformazione Digitale è oggi una priorità. È incoraggiante notare che, sempre dall'indagine effettuata, la postura di sicurezza delle aziende è costantemente migliorata negli ultimi anni, specialmente per quanto riguarda lo smart working e l'utilizzo dei servizi in cloud. Questo è in linea con le ultime tendenze lavorative, soprattutto dopo l'emergenza Covid-19. Tuttavia, ci sono ancora aree in cui è necessario migliorare, come la gestione dei dati, la relazione con i clienti, lo sviluppo di nuovi prodotti e l'integrazione tra IT (information technology) e OT (operational technology).



[figura - Capitolo Cyber – IMG3]

In particolare, l'Internet delle Cose (IoT) rappresenta un'area critica in cui è necessario concentrarsi per ridurre il gap di sicurezza. Molte aziende stanno ancora recuperando il terreno perso in termini di sicurezza nell'ambito dell'IoT, e ciò richiede un impegno significativo per applicare principi di security e privacy by design fin dalle fasi iniziali dei nuovi sviluppi digitali.

Un settore caratterizzato da ampia interconnessione tra oggetti, siti, realtà diverse ed eterogenee in ecosistemi complessi è quello industriale, che per l'ampia superfice d'attacco e le molte vulnerabilità, è stato purtroppo martoriato negli ultimi anni da attacchi mirati con conseguenze molto gravi. L'impennata della connettività e della condivisione di dati nell'ecosistema manifatturiero ha ampliato l'esposizione del settore, rendendolo a livello globale, per tre anni consecutivi, il più bersagliato da attacchi informatici, con una quota del 25,7% sul totale, e con il ransomware che costituisce il 71% di questi attacchi[1].

Gli attacchi informatici possono mettere in crisi le attività aziendali e le catene di approvvigionamento, vanificando i vantaggi della digitalizzazione e causando danni finanziari, di produttività, di reputazione persino danni fisici. In effetti, il 57% degli attacchi informatici effettuati

nel 2022 che prendevano di mira Operational technologies (OT) ha avuto conseguenze fisiche reali, tra cui: interruzioni alla produzione, incidenti che hanno danneggiato le apparecchiature, incidenti che hanno messo a rischio la sicurezza dei lavoratori sul campo[2]. Il ransomware rimane poi la principale preoccupazione per l'industria: il numero degli attacchi informatici rivolti al mondo industriale continua a crescere anno dopo anno. Nel corso del 2023, il numero degli attacchi ransomware all'infrastruttura industriale è raddoppiato, facendoli diventare una minaccia significativa, e i pagamenti del ransomware hanno raggiunto un valore record di 1,1 miliardi di dollari[3].

Date la complessità delle moderne supply chain, interruzioni lungo ampie catene del valore possono avere effetti a cascata, al di là del controllo effettuabile da parte di una singola realtà. Le complessità intrinseche della manifattura e delle supply chain richiedono quindi un approccio olistico alla mitigazione dei rischi informatici.

La cyber resilienza richiederebbe uno sforzo comune e coordinato

È evidente che per raggiungere un adeguato livello di cyber resilienza, è necessario uno sforzo collettivo e coordinato da parte di tutte le aree aziendali coinvolte. Tuttavia, al momento solo una minoranza delle aziende

ha posto l'accento sulla necessità di collaborare attivamente con tutte le aree di business per aumentare il controllo e migliorare la resilienza.

Per i responsabili della cybersecurity, ci sono diversi approcci chiave per migliorare la cyber resilienza della propria organizzazione. In primo luogo, l'importanza della formazione è ampiamente riconosciuta, con l'81% degli intervistati che ritiene che la formazione sia prioritaria per aumentare la consapevolezza e la preparazione del personale di fronte alle minacce informatiche.

Al secondo posto, la tempestività della risposta è considerata cruciale: il 73% ritiene che la capacità di rispondere prontamente agli attacchi informatici sia fondamentale per limitare i danni e ripristinare rapidamente le operazioni. Test e simulazioni sono poi diventati uno strumento indispensabile per verificare il livello di preparazione e identificare eventuali punti deboli nei sistemi e nei processi aziendali: la maggioranza degli intervistati (il 63%) ritiene che l'esecuzione regolare di test e simulazioni sia essenziale per mantenere un alto livello di preparazione e reattività.

Inoltre, la visibilità estesa e l'accesso alla threat intelligence sono considerati fattori cruciali per una strategia efficace di cyber resilienza. Il 55% degli intervistati ritiene che una visibilità estesa sui sistemi e sulle reti aziendali sia fondamentale per individuare e rispondere prontamente alle minacce informatiche, mentre il 53% sottolinea l'importanza di avere accesso a informazioni dettagliate sulle minacce informatiche attuali ed emergenti. Quest'ultimo aspetto, in particolare, permette di focalizzare gli sforzi sui rischi più gravi e quindi disegnare un programma di cybersecurity che punti alla massima efficacia nei risultati.

In sintesi, per migliorare la cyber resilienza, le aziende dovranno sempre di più concentrarsi sulla formazione del personale, sulla tempestività della risposta agli attacchi, sull'esecuzione di test e simulazioni regolari, sull'ottenimento di una visibilità estesa sui propri sistemi e sull'utilizzo della threat intelligence per identificare e mitigare le minacce informatiche in modo efficace. ■

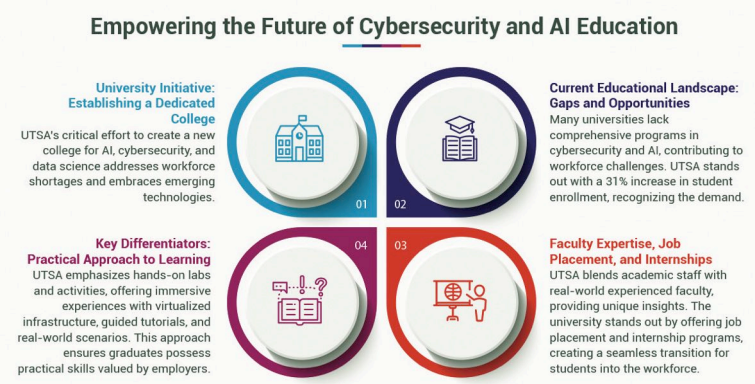
BIO

Nell'aprile 2012 Elena Vaciago si è aggiunta al Team di The Innovation Group per servizi di Market Analysis e supporto al Go-to-market. Laureata in Fisica Nucleare presso l'Università degli Studi di Milano nel 1992, ha iniziato la carriera occupandosi dell'analisi dei trend che caratterizzano il settore ICT collaborando con Il Sole 24 Ore come giornalista specializzata su queste tematiche, oltre che con l'Università Cattolica del Sacro Cuore di Milano, in qualità di Docente Universitario. Fino al 2004 ha partecipato in Università Cattolica a progetti formativi e di ricerca, con responsabilità sulla progettazione di corsi Master. Nel 2002, è stata responsabile del corso Universitario Post laurea "Internet Banking" organizzato dall'Università Cattolica per Banca Intesa BCI. Nel 2001 è entrata in IDC, società internazionale di ricerca, consulenza e analisi di mercato specializzata per l'ambito Informatica e Telecomunicazioni, come ricercatore di mercato. Elena Vaciago come Research Manager si occupa in The Innovation Group di attività di Ricerca di mercato, survey, pubblicazione di Studi e approfondimenti sui principali trend in ambito ICT, in parallelo con il piano annuale di eventi oltre che a supporto del Cybersecurity & Risk Management Leadership Program.

1 Dragos. (2024). 2023 OT Cybersecurity Year in Review. https://www.dragos.com/ot-cybersecurity-year-in-review/.
2 Waterfall Security. (2023) 2023 Threat Report – OT Cyberattacks With Physical Consequences. https://waterfallsecurity.
3 Chainalysis. (2024). 2024 Crypto Crime Trends: Illicit Activity Down as Scamming and Stolen Funds Fall, But Ransomwareand Darknet Markets See Growth. https://www.chainalysis.com/blog/2024-crypto-crime-report-introduction/.

Le sfide delle Academy e le Risorse Umane nella Cyber Security aziendale.

Autore: Italo Piroddi



In un'era di crescente digitalizzazione, le aziende si trovano ad affrontare sfide sempre più complesse nel campo della sicurezza informatica. Le minacce cyber sono in continua evoluzione e richiedono un approccio proattivo e integrato per proteggere i dati sensibili e garantire la continuità operativa. In questo contesto, le Academy e le Risorse Umane svolgono un ruolo cruciale nel gestire professionisti competenti e aggiornati.

Le sfide delle Academy

Le Academy sono chiamate a fornire una formazione di alta qualità, in grado di rispondere alle esigenze del mercato e alle sfide della Cyber Security.

Tra le principali sfide:

- aggiornamento continuo dei programmi formativi che devono mantenersi al passo con l'evoluzione delle minacce e delle tecnologie. Ciò richiede una stretta collaborazione con i professionisti del settore e una costante attività di ricerca e analisi delle tendenze;
- instaurare partnership solide con gli esperti di Cyber Security, per fornire una formazione mirata e applicabile. Le Academy possono offrire programmi di stage, progetti di ricerca congiunti;
- promozione di competenze trasversali, oltre alle competenze tecniche. Le Academy devono promuovere lo sviluppo di soft skill, come il pensiero critico, la comunicazione efficace e il lavoro di squadra: queste competenze sono essenziali per affrontare le sfide complesse della Cyber Security e lavorare efficacemente in team multidisciplinari;
- accessibilità e flessibilità per offrire percorsi formativi flessibili e accessibili, sfruttando le potenzialità della formazione digital e blended (e oramai dell'AI). Ciò consente di raggiungere un pubblico più ampio e di venire incontro alle esigenze di studenti e professionisti con impegni lavorativi e familiari;
- formazione continua per promuovere una cultura della Security Awareness. Ciò include anche l'organizzazione di workshop interni, la sponsorizzazione della partecipazione a conferenze e seminari, e il supporto per il conseguimento di certificazioni riconosciute a livello internazionale, come CISSP, CISM e CompTIA Security+.

Il ruolo delle Risorse Umane

Le Risorse Umane sono il ponte tra le Academy e l'organizzazione, con il compito di attrarre, selezionare e trattenere i talenti nella Cyber Security.

Le sfide principali includono:

- identificazione delle competenze chiave collaborando con i responsabili della sicurezza IT per identificare le competenze critiche necessarie all'azienda. Ciò richiede una profonda comprensione delle

esigenze di business e delle minacce cyber specifiche del settore in cui opera l'organizzazione;

- attrarre i talenti, in quanto un mercato competitivo, le HR devono sviluppare strategie efficaci per attrarre professionisti qualificati e motivati. Ciò può includere la partecipazione a eventi di settore, la collaborazione con le università e le Academy, e l'offerta di pacchetti retributivi e di benefit attrattivi;
- retention dei talenti sviluppando piani di carriera e sistemi di reward per trattenere i professionisti più talentuosi e prevenire il turnover. Le HR possono implementare programmi di mentoring, offrire opportunità di crescita interna e riconoscere i risultati eccezionali con premi e bonus.

Collaborazione e sinergie

Per affrontare efficacemente le sfide della Cyber Security, è fondamentale promuovere la collaborazione e le sinergie tra Academy, Risorse Umane e altri stakeholder.

Academy aziendali, HR e professionisti del settore devono condividere best practice, esperienze e insight per migliorare continuamente la formazione e la gestione dei talenti. Ciò può avvenire attraverso la partecipazione a forum online, gruppi di lavoro tematici e iniziative di knowledge sharing.

La collaborazione tra Academy, aziende, istituzioni e centri di ricerca può favorire l'innovazione e lo sviluppo di soluzioni avanzate.

Inoltre, Academy e HR possono contribuire a diffondere una cultura della sicurezza informatica a tutti i livelli dell'organizzazione, coinvolgendo anche i non specialisti. Ciò può includere campagne di sensibilizzazione, workshop dedicati e l'integrazione di moduli di Cyber Security nei programmi di onboarding per i nuovi dipendenti.

Tendenze future e prospettive

Guardando al futuro, le Academy e le Risorse Umane dovranno affrontare sfide sempre più complesse nella Cyber Security.

Alcune delle tendenze chiave includeranno:

- intelligenza artificiale e machine learning da integrare nei processi formativi, fondamentali per preparare i professionisti ad affrontare minacce sempre più sofisticate e automatizzate;
- gestione del rischio cyber grazie alle Academy che dovranno fornire competenze avanzate in ambito di risk management, consentendo ai professionisti di valutare, prioritizzare e mitigare i rischi cyber in un contesto di business in continua evoluzione;
- reskilling e upskilling, in quanto con il rapido evolversi delle minacce e delle tecnologie, sarà cruciale garantire un aggiornamento costante delle competenze dei professionisti della Cyber Security. Le HR dovranno implementare programmi di formazione continua e supportare l'acquisizione di nuove certificazioni.

Solo attraverso un impegno congiunto tra Academy, HR, aziende, istituzioni e centri di ricerca e una visione condivisa, sarà possibile formare le nuove generazioni di professionisti della Cyber Security e garantire la resilienza delle organizzazioni di fronte alle minacce informatiche.

Concludo con una riflessione: le sfide della Cyber Security richiederanno un impegno costante e sinergico da parte di Academy e le Risorse Umane. Solo attraverso la formazione di alta qualità, la gestione strategica dei talenti e la collaborazione diffusa sarà possibile costruire organizzazioni resilienti e pronte ad affrontare le minacce del presente e del futuro.

Dovranno fornire programmi formativi aggiornati, promuovere competenze trasversali e garantire accessibilità e flessibilità. Le Risorse Umane, d'altra parte, devono identificare le competenze chiave, attrarre e trattenere i talenti, e promuovere una cultura dell'apprendimento continuo.

La collaborazione tra Academy, HR e altri stakeholder, attraverso la condivisione di conoscenze, i partenariati strategici e la sensibilizzazione, sarà fondamentale per affrontare le sfide future della Cyber Security, che includeranno l'Intelligenza Artificiale, la sicurezza delle infrastrutture critiche e la gestione del rischio cyber.

Investire nelle persone e nelle loro competenze è la chiave per garantire la sicurezza e il successo delle aziende nell'era digitale. Solo attraverso un impegno congiunto e una visione condivisa sarà possibile costruire un futuro digitale più sicuro e resiliente per tutti. ■

BIO

In un mondo in cui l'innovazione è all'ordine del giorno, c'è una persona che si distingue per la sua capacità di mantenere vive le competenze. Il suo nome è Italo Piroddi, l'HR Training Manager che sta ridefinendo le regole del gioco. Non è solo un manutentore di competenze, ma un vero e proprio custode della conoscenza. Dotato di una sete insaziabile di apprendimento, Italo è sempre alla ricerca di nuove sfide e nuovi orizzonti da esplorare. Ma non è tutto lavoro e niente gioco: quando il sole cala, Italo si rifugia nel suo mondo privato, un mondo costruito di parole e storie, un mondo che si apre ogni volta che apre un libro. La lettura è la sua passione, la sua fuga, il suo rifugio, così come la musica è la sua fonte d'ispirazione. Quando Italo non sta plasmando le menti di domani, si perde nelle melodie delle sue dieci chitarre, che danno vita ai suoi sogni. Italo, un manutentore di competenze, un apprendista perenne, un amante dei libri con la forza di un leader e il cuore di un musicista. Questo è il suo mondo. Questo è Italo.

Direttiva NIS2: le sfide per le imprese italiane.

Autori: Lorenzo Russo e Franceso Binaschi

Introduzione

La direttiva **NIS2** ***"Network and Information Security"*** è la normativa del Parlamento Europeo e del Consiglio relativa a misure per un livello comune di cybersicurezza nell'Unione Europea, entrata in vigore il 17 gennaio 2023.

BIO

Lorenzo Russo è Partner di Deloitte Risk Advisory con esperienza di oltre 25 anni in ambito Cyber Security Strategy, Governance & Risk Management, maturata in progetti con governi, organizzazioni internazionali e aziende Fortune 500. Co-autore del Framework Nazionale per la Cyber Security e del NATO Next Generation CERTs Handbook e Advisor delle UN per temi di National Cyber Strategy e Capacity Building. In Deloitte è responsabile dell'Offering Cyber Strategy and Trasformation per il settore industriale.

BIO

Francesco Binaschi è Senior Manager di Deloitte Risk Advisory con esperienza di 10 anni in ambito Cyber Security Strategy, Governance & Risk Management, e Compliance maturata in progetti con infrastrutture critiche, organizzazioni internazionali e PMI italiane. Responsabile dei servizi Deloitte di Compliance alle Direttive Europee e Leggi Nazionali sulla Cyber Security e Cyber Resilience (NIS, PSNC, CER, …)

La NIS2 abroga la precedente direttiva NIS1 e ha l'obiettivo di rafforzare la resilienza e la sicurezza delle reti e dei sistemi informativi in tutti gli Stati Membri dell'Unione Europea.

La NIS2 si applica a numerosi settori come l'energia, i trasporti, le banche, le infrastrutture dei mercati finanziari, la sanità, (incluso quello farmaceutico), la fornitura di acqua potabile e le infrastrutture digitali, il cloud e l'ICT Service Provider, la Pubblica Amministrazione e lo spazio; identificati come **settori ad alta criticità** nell'**allegato** I della direttiva[1]. A questi si aggiungono nuovi settori critici descritti nell'allegato II della direttiva, ovvero: chimica, gestione dei rifiuti, fabbricazione/manifatturiero, produzione, trasformazione e distribuzione di alimenti, servizi postali e di corriere, fornitori di servizi digitali e ricerca.

La direttiva stabilisce che un soggetto – impresa pubblica o privata - possa rientrare nell'ambito della NIS2 se opera in almeno uno dei settori elencati negli Allegati e superare le soglie di *Size Cap* definite dall'UE, qualificando si **almeno come media impresa** ai sensi della raccomandazione della Commissione europea 2003/361/CE del 6 maggio 2003. In tal caso, l'impresa dovrà **auto-dichiararsi come soggetto NIS** presso lo Stato di residenza.

L'iter normativo della direttiva NIS2 prevede il recepimento da parte di tutti gli Stati Membri in una Legge nazionale entro il 17 ottobre 2024. Nell'ambito del recepimento ogni Paese identificherà poi la data ultima entro cui ciascuna impresa dovrà auto-dichiararsi come **soggetto essenziale** o **importante**, a seconda della sua dimensione e del settore in cui opera. Tale differenziazione comporta un **regime di supervisione** (i.e. ex ante vs ex post) **e sanzioni differenziati** e, a discrezione dei singoli Stati Europei, possibili distinzioni anche in termini di misure di sicurezza richieste.

Nuovi obblighi e principali elementi di prescrizione

La nuova direttiva NIS2 rappresenta un passo significativo verso un ecosistema digitale più sicuro e armonico all'interno dell'Unione Europea. Volendo analizzare i nuovi elementi introdotti con più diretto impatto sui soggetti coinvolti[2], in primo luogo, le organizzazioni dovranno implementare **misure di gestione del rischio Cyber più rigorose con riferimento a tutti gli Asset aziendali**, sia in ambito IT che OT (i.e. a differenza della direttiva NIS1, che si applicava unicamente agli Asset a supporto dei servizi più critici), come ad esempio: sicurezza della catena di approvvigionamento, continuità operativa, gestione degli incidenti e strategie per valutare l'efficacia delle misure di gestione del rischio Cyber. Ai soggetti cui si applica la direttiva viene richiesto di valutare la criticità di tutti gli Asset aziendali, al fine di implementare misure di gestione del rischio Cyber secondo una modalità Risk-based.

Inoltre, la direttiva NIS2 prevede che gli **organi di gestione** dei soggetti che rientrano nell'ambito di applicazione della stessa, ricoprano un ruolo attivo nella definizione e supervisione della strategia di gestione del rischio Cyber dell'organizzazione, e siano responsabili per la propria formazione e per quella di tutti i dipendenti su rischi e minacce Cyber.

Anche il tema della sicurezza lungo tutta la **Supply Chain** ricopre un ruolo fondamentale all'interno della direttiva: le imprese dovranno introdurre processi per verificare l'adeguatezza dei fornitori e delle relative forniture da un punto di vista Cyber, nonché garantire un monitoraggio continuo dei rischi Cyber che una terza parte può veicolare nel corso del contratto, ad esempio eseguendo audit periodici.

In aggiunta, la direttiva prevede obblighi più stringenti in materia di **segnalazione e gestione degli incidenti** informatici: i soggetti devono provvedere a inviare un preallarme entro 24 ore dal momento in cui vengono a conoscenza di un incidente significativo ed entro 72 ore una notifica dell'incidente che aggiorni le informazioni già trasmesse; entro un mese, i soggetti sono tenuti a inviare un report finale con l'analisi dell'incidente.

Da ultimo la direttiva prevede un regime di supervisione, che in Italia sarà in capo all'Agenzia per la Cybersicurezza Nazionale. L'Agenzia agirà come autorità NIS e sarà responsabile per le attività di vigilanza sulle imprese e sanzioni. La direttiva prevede infatti che la mancata Compliance potrebbe comportare **sanzioni** che possono arrivare fino a 10 Milioni di euro o 2% del fatturato annuo globale dell'organizzazione per i soggetti essenziali, e fino a 7 Milioni di euro o 1.4% del fatturato annuo globale dell'organizzazione per i soggetti importanti.

Le sfide per le imprese rientranti in NIS2

La direttiva NIS2 pone in capo alle aziende pubbliche e private coinvolte numerose sfide per garantire la conformità. Sfide che sono state precedentemente affrontate per la conformità alla direttiva NIS1 – delle quali nuovi soggetti possono far tesoro – ma nuove sfide determinate ad esempio

all'eterogeneità dei settori che ricadono in ambito o alla complessità attuativa richiesta per l'adozione di misure di sicurezza. Analizziamo le principali:

Chiara identificazione dell'ambito – la direttiva NIS2 prevede che le imprese si auto-dichiarino (differentemente dalla NIS1 che prevedeva una nomina diretta) come soggetti essenziali o importanti. Ciò comporterà un impegno non indifferente per quelle realtà come i gruppi e le società multi-Business o anche i gruppi internazionali, per i quali sarà necessario analizzare - a livello nazionale ed europeo - sia i settori di appartenenza delle singole società del Gruppo, ma anche la dimensione in termini di dipendenti e fatturato o bilancio annuo (i.e. tenendo conto potenzialmente anche di società collegate e/o associate), in accordo con la Raccomandazione 2003/361/CE.

Approcci e tempistiche di conformità differenti – la direttiva NIS2 pur avendo l'obiettivo lodevole di definire il livello comune di cybersicurezza nell'Unione Europea lascia comunque agli Stati membri la libertà di definire specifiche modalità e tempistiche di attuazione, con potenziali implicazioni in termini di armonizzazione a livello comunitario. I gruppi internazionali dovranno gestire diversi approcci, (e.g. per implementazione delle misure di cybersicurezza o per la notifica degli incidenti) - e tempi di conformità che potranno variare a seconda del paese in cui operano.

Analogamente all'interno di un singolo paese, ci potranno essere potenzialmente società appartenenti a gruppi multi-Business chiamate ad ottemperare ai requisiti previsti per i soggetti essenziali e altre invece a quelli previsti per gli importanti. Il condizionale è d'obbligo in quanto non è ancora definito se effettivamente una differenziazione - secondo il principio di proporzionalità - tra le misure richieste ai soggetti essenziali e importanti, o tra gli stessi soggetti appartenenti ad uno dei due gruppi, sarà definita a livello nazionale. Saranno da vagliare infatti le implicazioni associate alle differenze tra settori, ma anche quelle tra soggetti all'interno dei singoli settori.

Governance della Compliance – come per la direttiva NIS1, la conformità alla direttiva comporta per i

gruppi ulteriori sfide in termini di definizione dei modelli di governance, dei livelli e criteri di Accountability fino a spingersi alla formalizzazione di procure per indirizzare e gestire inizialmente la conformità all'interno dell'organizzazione ma poi riuscire a controllarla e monitorarla con continuità nel tempo. L'esperienza nell'assicurare la conformità alle precedenti direttive e/o leggi indica come un modello di governo sia indispensabile per assicurare che tutti gli attori coinvolti all'interno delle organizzazioni si impegnino in maniera continuativa nell'attuazione delle disposizioni.

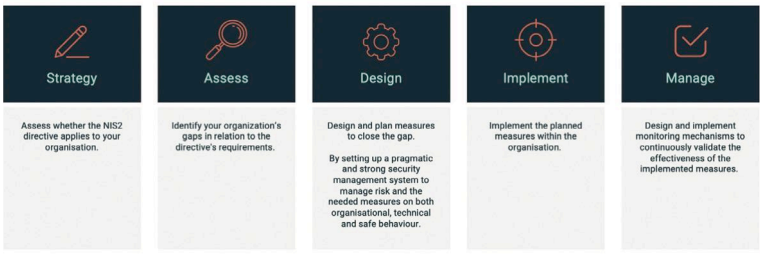
Multidisciplinarità degli attori coinvolti – la conformità al quadro normativo richiede interventi che hanno implicazioni e impatti che non sono esclusivamente di carattere tecnico o specificamente di Cybersecurity ma che vedono coinvolti numerosi altri Stakeholder aziendali come ad esempio Procurement, IT, Operations OT, HR, Legal, Compliance. La sfida è quella di coinvolgere con l'adeguato Commitment tutti questi interlocutori e coordinarli nel tempo in maniera efficace ed efficiente.

Complessità per implementazione delle misure di sicurezza su tutti i sistemi IT e OT – l'estensione dell'ambito di applicabilità a tutti gli asset aziendali, a differenza della NIS1 che circoscriveva unicamente alle risorse informatiche e ai servizi critici, implica un importante estensione di ambito per tante imprese che erano già in NIS1, ma soprattutto comporta un importante impegno per tutti i numerosi nuovi operatori NIS2. L'adozione delle misure di sicurezza sarà guidata dai principi di proporzionalità e adeguatezza direttamente richiamati dalla direttiva, che richiederanno alle imprese coinvolte di:

- completare valutazioni di impatto (i.e. BIA) su tutta l'organizzazione al fine di differenziare i sistemi in ragione della loro criticità;
- definire, implementare e monitorare l'efficacia di soluzioni tecniche, organizzative, di processo adottate per rispondere alle misure richieste in maniera differenziata sulla base del rischio, sia sugli ambienti IT che su quelli OT.

Entrambe le attività potranno risultare complesse in termini tecnici, di commitment e di risorse. Questo in particolare per imprese di medie dimensioni, con un livello di maturità iniziale in ambito Cybersecurity, ma anche per le grandi imprese che avranno un perimetro più ampio di conformità da gestire.

La possibilità di adottare principi di **gradualità** - che permettano ad esempio di prevedere in una prima fase misure e tempistiche per i sistemi e reti o i servizi critici che il singolo soggetto fornisce, lasciando ad una successiva fase l'obbligo di adottare misure e tempi differenziati per il restante insieme dei servizi e sistemi appartenenti al soggetto; **flessibilità** - nel lasciare al soggetto la libertà di adozione di metodologie e approcci per la differenziazione dei sistemi all'interno di un'organizzazione su cui applicare le misure di sicurezza o per la definizione, implementazione e verifica di efficacia delle soluzioni, potranno agevolare l'adozione bilanciando obiettivo e fattibilità.



Come prepararsi per il recepimento della direttiva

Per essere adeguatamente preparate agli obblighi cogenti imposti dalla direttiva NIS2 e all'ormai imminente recepimento di quest'ultima nel nostro ordinamento nazionale, le imprese possono intraprendere alcune azioni preparatorie.

La direttiva NIS2 richiede una **comprensione** del **contesto societario** e **operativo** dell'impresa. Questo, all'atto pratico, impone un'analisi della struttura societaria, delle attività operative effettuate più che aspetti di carattere quantitativo, come numero di dipendenti e fatturato. Inoltre, è essenziale **identificare** e **valutare** i **processi** e le risorse informatiche che sottendono i servizi forniti dai soggetti.

Passo successivo è quello di **valutare** poi il proprio **livello** di **aderenza** ai requisiti oggi delineati nella direttiva NIS2, con lo scopo di cogliere differenze presenti fra le varie società o aree di business dell'impresa, così come **identificare** per tempo eventuali **gap**, in particolare nell'area OT, storicamente più legacy. L'obiettivo finale è quello di **definire** e **implementare** un **programma** di adeguamento mirato e sostenibile.

Compreso ambito e maturità la conformità deve poter essere affrontata con **approccio programmatico** che identifichi puntualmente ruoli e responsabilità di tutti gli Stakeholder aziendali chiamati a contribuire al processo di adeguamento e al suo mantenimento nel tempo. In tal senso sarà cruciale definire in maniera chiara un **modello di governo** che formalizzi ruoli e le responsabilità di ciascun attore aziendale nei processi di adeguamento NIS2.

Conclusioni

La direttiva NIS2 rappresenta di fatto un'opportunità per incrementare ulteriormente la propria postura Cyber, valorizzare il ruolo della cybersecurity nel processo di trasformazione digitale e accrescere la fiducia di clienti, partner e istituzioni. Dall'altro lato, come visto, presenta anche notevoli sfide per tutto l'ecosistema di imprese europee, che impongo un approccio programmatico e strutturato per la conformità. ■

1 Per l'elenco completo dei settori e relativi sottosettori, si vedano gli Allegati I e II della Direttiva https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32022L2555

2 Ad esempio la regolamentazione per la divulgazione coordinata delle vulnerabilità (CVD) e le specifiche funzioni di coordinamento attribuite a CSIRT nazionali; oppure l'implementazione delle misure di cooperazione, al fine di sostenere la gestione coordinata a livello operativo degli incidenti e delle crisi di cybersicurezza su vasta scala.

Il processo di attuazione della NIS 2 in Italia.

Autore: **Erik Longo***

Entro il 17 ottobre 2024 l'Italia dovrà adeguare il suo ordinamento alla Direttiva NIS 2. Quest'ultima ha tre grandi pretese. Anzitutto, aumentare la capacità degli Stati membri in termini di architettura istituzionale, strategia nazionale e piani di gestione delle crisi cibernetiche. In secondo luogo, intervenire nella gestione del rischio da parte degli operatori con misure di sicurezza adeguate e un sistema di notifica degli incidenti che sia efficace e reattivo. In terzo luogo, incentivare la cooperazione e la condivisione delle informazioni, attraverso diverse modalità di scambio, a livello europeo e nazionale.

Nel momento in cui è stata approvata la legge 21 febbraio 2024, n. 15, "Legge di delegazione europea 2022-2023", sulla base della quale il Governo dovrà emanare uno o più decreti delegati entro la data di scadenza indicata dalla Direttiva NIS 2 per il recepimento delle nuove norme in materia di cybersicurezza.

Dall'esame del disegno di legge delega si comprende che, come accade in queste circostanze, insieme ai princìpi e criteri direttivi generali di cui all'art. 32, legge n. 234/2012, il legislatore ne ha previsti di ulteriori e più specifici relativi all'ambito della delega. Tali previsioni hanno una rilevanza notevole per il nostro esame.

Il *primo* gruppo di criteri che il decreto delegato dovrà seguire concernono i soggetti della pubblica amministrazione da sottoporre alle nuove regole. Il rischio *cyber* a cui sono sottoposte le amministrazioni è di particolare importanza e anche di recente è stato disciplinato dal legislatore con riguardo agli effetti della guerra russo-ucraina. Per quanto riguarda l'attuazione della NIS 2, il Governo dovrà anzitutto individuare i criteri in base ai quali un ente pubblico può essere considerato pubblica amministrazione ai fini dell'applicazione delle disposizioni della direttiva e poi definire tanto le esclusioni di particolari soggetti, gli enti della pubblica amministrazione operanti nei settori di cui all'art. 2, paragrafo 7, della direttiva medesima, quanto avvalersi della facoltà prevista per gli Stati membri dall'art. 2, paragrafo 8, della Direttiva.

Il *secondo* gruppo di criteri concerne i soggetti che si occupano della cybersicurezza a livello centrale. Qui vi sono sia le norme che richiedono la conferma della distinzione tra l'Agenzia per la cybersicurezza nazionale, quale autorità nazionale competente e punto di contatto, ai sensi della direttiva (art. 8), e le autorità di settore operanti negli ambiti di cui agli allegati I e II alla medesima Direttiva, sia le norme in attuazione dell'art. 10 relativo alla

BIO

Erik Longo è professore associato di Diritto Costituzionale presso il Dipartimento di Scienze Giuridiche dell'Università degli Studi di Firenze. Nella stessa Università insegna Istituzioni di Diritto Pubblico, Rights and Rules for Artificial Intelligence, Diritto della Privacy.

***L'intervento che pubblichiamo per gentile concessione dell'Editore Giappichelli è tratto dal capitolo "La disciplina della Cybersicurezza nell'Unione europea e in Italia"; contenuto nel volume: "La regolazione europea della società digitale".**

istituzione dello CSIRT Italia, nonché l'ampliamento di quanto previsto dal medesimo decreto relativamente alla collaborazione tra tutte le strutture pubbliche coinvolte in caso di eventi malevoli alla sicurezza informatica.

Il *terzo* gruppo di criteri attiene ai destinatari delle nuove norme. Qui il legislatore delegato dovrà non solo descrivere il regime transitorio per i soggetti già sottoposti alla disciplina del d.lgs. n. 65/2018 ai fini della applicazione delle disposizioni previste dalla Direttiva NIS 2 , ma anche prevedere meccanismi che consentano la registrazione dei soggetti essenziali e importanti ai fini della comunicazione dei dati previsti dal paragrafo 4 dell'art. 3. In base alle nuove regole della direttiva, gli Stati membri devono definire entro il 17 aprile 2025 un elenco dei soggetti essenziali e importanti nonché dei soggetti che forniscono servizi di registrazione dei nomi di dominio, da riesaminare e aggiornare ogni due anni.

Il *quarto* – e più delicato – gruppo di criteri riguarda l'introduzione di modifiche necessarie alla legislazione vigente, anche in materia penale, per assicurare il recepimento nell'ordinamento nazionale delle disposizioni della Direttiva NIS 2 in tema di divulgazione coordinata delle vulnerabilità. La nuova direttiva stabilisce un quadro per la divulgazione coordinata delle vulnerabilità (art. 12), che consiste in un processo strutturato attraverso il quale queste ultime sono segnalate al fabbricante o al fornitore dei prodotti e servizi digitali potenzialmente, in modo tale da consentire loro di diagnosticarle ed eliminarle prima che informazioni dettagliate in merito siano divulgate a terzi o al pubblico.

Il *quinto* gruppo attiene ai sistemi sanzionatorio, di vigilanza ed esecuzione previsti dal d.lgs. n. 65/2018. In proposito, si dispone un primo specifico criterio di delega che prevede che le nuove sanzioni siano effettive, proporzionate e dissuasive rispetto alla gravità della violazione degli obblighi derivanti dalla Direttiva NIS 2, "anche in deroga ai limiti previsti dall'art. 32, comma 1, lettera d), della legge n. 234/2012 e alla legge n. 689/1981" e si indica l'introduzione di strumenti deflattivi del contenzioso.

Infine, il legislatore delegato è chiamato ad assicurare il coordinamento tra le disposizioni della Direttiva NIS 2, della Direttiva CER, del Regolamento DORA e della direttiva in materia di servizi finanziari, le cui deleghe sono contenute in altri articoli della medesima proposta.

Va, infine, menzionato il fatto che nel febbraio 2024 il Governo italiano, ha presentato alla Camera dei Deputati un disegno di legge contenente norme sul rafforzamento della cybersicurezza nazionale e l'inasprimento delle pene per i reati informatici. Le nuove disposizioni rispondono proprio

alla necessità, oggi sempre più impellente, di far emergere in modo più puntuale misure capaci di prevenire, analizzare e rispondere gli incidenti di sicurezza informatica e gli attacchi informatici diretti alle pubbliche amministrazioni oggi non comprese nel Perimetro di sicurezza nazionale cibernetica. Tali previsioni risultano sempre più importanti e opportune nell'ottica del recepimento della Direttiva NIS 2 e del connesso cambio di prospettiva che sarà richiesto sia al settore pubblico sia al settore privato.

La disciplina della cybersicurezza tra fattori materiali e immateriali

L'evoluzione della sicurezza cibernetica ha seguito una dinamica sempre più rivolta a realizzare una convergenza tra fattori materiali e immateriali. Le norme approvate dimostrano che nel tempo la *cybersecurity* ha assunto delle caratteristiche nuove. Oggi, infatti, l'esigenza di garantire risposte veloci e resilienti alle molteplici minacce alla sicurezza richiede la protezione degli strumenti digitali con i quali si governa sia l'erogazione dei servizi pubblici sia le catene di produzione e il mercato dei beni e servizi. Non esiste più una dimensione della sicurezza avulsa dagli strumenti tecnologici, avendo oramai le nostre vite acquisito una forma "nuda" che implica necessariamente il digitale .

Gli ultimi anni segnano un allargamento notevole del concetto di *cybersecurity*. Da essere solo l'insieme di "tecnologie, programmi, processi e tecniche (anche sociali) concepiti e messi in atto per proteggere dispositivi, dati e reti informatiche" a elemento al centro della vita digitale. Il passaggio è notevole.

Difatti, per garantire la *cybersecurity* oggi è necessario sempre più investire in un livello alto di *cyber-resilience*. Ne sono un segnale sia

l'evoluzione tecnologica sia le trasformazioni della governance stessa di questo fenomeno che oggi vede una sempre maggiore interconnessione tra soggetti privati e pubblici.

Il concetto di resilienza tratta gli eventi informatici avversi come parte delle normali operazioni di tali sistemi. La differenza con un approccio solo securitario è cruciale perché spinge le organizzazioni a incorporare le contromisure, i piani di emergenza e le stesse tecnologie come parte di quella che potrebbe essere considerata una "nuova normalità". Il concetto di resilienza applicato alla *cybersecurity* coglie quella natura multidimensionale e multidisciplinare che è necessaria per amalgamare fattori tecnologici, sociali, economici, aziendali e culturali e rendere l'uso del digitale più sicuro.

Possedere e sollecitare livelli di sicurezza informatica più elevati è essenziale per stabilire la fiducia senza la quale la società digitale non può funzionare. Perciò, non può più essere considerata un *optional*, ma deve essere vista come un'esigenza sociale essenziale e un bene di tutti.

Se il cyberspazio è un bene comune e il suo governo un problema politico, cioè di tutti, sono richieste forme di regolamentazione e tutela che non possono essere lasciate nelle mani dei soli attori economici o tecnologici dei settori interessati. La difesa di tali ambiti deve alimentarsi di un progressivo allineamento tra interessi privati e interessi pubblici e di una convergenza verso l'obiettivo della sicurezza *tout court*, intesa in senso olistico proprio come un bene *di* e *per* tutti.

Gli ultimi atti normativi adottati o in fase di approvazione dall'Unione europea assumono un approccio alla *cybersecurity* intesa come parte del più generale impegno del potere politico, insieme ai soggetti privati, ad assicurare una disciplina della tecnologia informatica che garantisca il rispetto delle regole necessarie alla sopravvivenza della democrazia e dei valori costituzionali.

Il cammino è però ancora tutto da compiere. Nonostante la maturata consapevolezza di tale passaggio, sempre più spesso ci troviamo di fronte a un atteggiamento che percepisce la sicurezza della società digitale come una questione riservata alle istituzioni statali, europee e internazionali, mentre oggi l'investimento nella cybersicurezza è divenuto un dovere di tutti. ■

Difendiamo il pluralismo delle narrazioni per ricostruire i "sentieri interrotti".

Intervista VIP con Marco La Rosa.

Autore: Massimiliano Cannata

Sono molte le suggestioni che offre la lettura di ***"Neuroscienze della narrazione"*** (ed. Hoepli). Se le organizzazioni produttive si dimostrassero "permeabili" rispetto ai messaggi e alle strategie di innovazione suggerite da Marco La Rosa, blogger e divulgatore scientifico attivo e originale frequentatore dei sentieri della comunicazione digitale, probabilmente ne potrebbero trarre un significativo vantaggio. Il metodo usato dallo scrittore è quello della "complessità", impossibile pensare di attuare una *reductio ad unum*, perché su determinati argomenti non può esistere una separazione delle discipline. Il crocevia delle problematiche connesse alla transizione digitale, non è appannaggio di alcuni, è l'intera società nel suo complesso che è in gioco. Esiste una dialettica irrisolvibile tra innatisti ed empiristi. Nel nostro DNA sono contenuti alcuni indizi decisivi del percorso futuro, ma non c'è dubbio che l'esperienza e il confronto ambientale e relazionale interviene a completare il profilo del soggetto. Quello che preme sottolineare, mentre assistiamo all'esplosione dell'intelligenza generativa, è il risorgere di posizioni pro e anti Cartesio come scrive Antonio R. Damasio nell'*"errore di Cartesio": "non esiste una ragione pure scevra da sentimenti, le emozioni non sono degli intrusi dentro le mura della ragione".* Sarebbe importante che questa consapevolezza entrasse nelle menti di chi per mestiere fa business e che sta ripensando l'impresa tenendo conto del mutamento economico e ambientale che segna la contemporaneità. La narrazione, il bisogno di creare storie nasce proprio da divenire socio – tecnologico che illumina la nostra epoca. Scrivere, narrare può essere una terapia per guardare al futuro con fiducia? Cybersecurity Trends ne ha parlato con l'autore.

Narrazione e neuroscienze in che cosa risiede l'importanza di questo connubio nella società digitale in cui viviamo immersi?

Le neuroscienze sono l'unico contributo che può aiutarci a comprendere il potere che esercitano le narrazioni su di noi e quindi una loro conoscenza di base può aiutarci a trasformare le storie da condizionamento a terapia, e a farci meno influenzare da narratori, imbonitori e persuasori di ogni sorta.

BIO

Marco La Rosa è uno scrittore, blogger e divulgatore scientifico. Da sempre attento alle tematiche dell'innovazione, nel 2019 ha fondato neurowbecopywriting.com, il primo blog italiano interamente dedicato all'applicazione delle neuroscienze cognitive alla comunicazione. Ha pubblicato per Hoepli (febbraio 2024) il libro: *Neuroscienze della narrazione, lo storytelling nell'era delle neuroscienze e dell'intelligenza artificiale,* con prefazione del professore Stefano Calabrese, e *Neurocopywriting* (2021), dedicato alla creazione dei contenuti.
Sito ufficiale: https://www.neurowebcopywriting.com

"La narrazione è una terapia", come Lei diceva in una recente intervista. Sembra un controsenso la ricerca della narrazione in un universo che tende ad asciugare il linguaggio, spesso compresso nelle strettoie di un Tweet. Come si spiega questo bisogno di rifondare un percorso di senso sul libero flusso del linguaggio narrato?

Vorrei precisare che la narrazione può rappresentare una terapia efficace in un contesto linguistico ricco e strutturato. Proprio le neuroscienze hanno scoperto il valore e la cifra in termini di benessere di discipline, quali la letteratura e, più in generale, i saperi umanistici. L'impoverimento linguistico e la riduzione dell'universo cogitante delle persone, rischia di distruggere le narrazioni e impoverendo le menti di chi subisce questo processo di "espoliazione" delle facoltà superiori, mi si passi il termine. Tutto questo apre la strada a riflessioni assai ampie, ad esempio l'interesse delle collettività a difendere la qualità, la ricchezza, la diversità e il pluralismo delle narrazioni che attraversano la società. L'educazione, la cultura, fattori decisivi, per preservare le capacità mentali e cognitive di tutti i componenti del corpo collettivo.

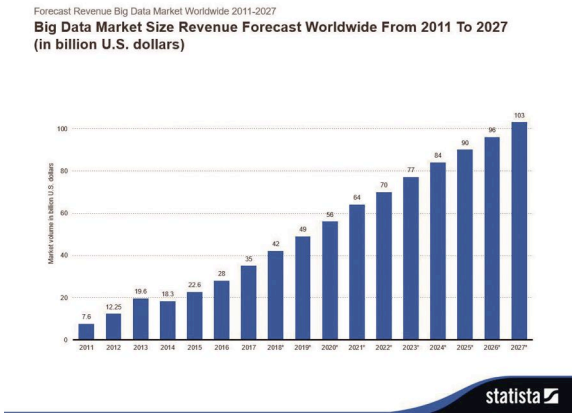
Intelligenze generative e narrazione, su questo aspetto è giustamente puntata l'attenzione di molti. Verso quale direzione stiamo andando?

Probabilmente stiamo andando verso una direzione di maggior standardizzazione, basti analizzare le immagini create con l'intelligenza artificiale, che trovo piuttosto simili e uniformate. Non bisognerebbe stupirsi, avviene questo da quando esiste l'industria: la standardizzazione c'è stata anche con la nascita della produzione di massa, e ha ispirato artisti come Andy Wharol e correnti come la pop art. Difficile dire come gli umani reagiranno: l'intelligenza generativa amplifica molte possibilità, ci sono aspetti positivi che non vanno sottovalutati. Non bisogna mai stancarsi di ribadirlo: l'AI è una componente neutra come tutte le tecnologie, dipende da chi la utilizza. Le persone con una buona cultura e senso critico sapranno coglierne le possibilità. Il rischio più grande rimane quello di una profonda spaccatura della società, tra chi sa cogliere i vantaggi morali e materiali dell'innovazione e chi rimane ai margini del progresso, che subisce e si impoverisce. Il vero alert di questo cambiamento d'epoca si chiama infatti sperequazione.

Il dato come asset sociale

L'economia dei dati cresce a ritmi vertiginosi. Il "dato è un asset sociale" come ha scritto Michele Mezza, a queste condizioni non Le pare che diventi utopistica la tutela di quello che Rodotà definiva "il corpo elettronico"?

I pericoli dell'economia dei dati sono ormai ben conosciuti e si riassumono nel rischio del grande fratello. Sul fronte della sicurezza, che rimane una delle grandi questioni del nostro tempo, Pierguido Iezzi (una delle personalità intervistate che arricchiscono il volume, n.d.r.) sottolinea la crescita di nuovi profili di rischio. Pensiamo all'identità digitale, video costruiti con l'AI in cui vengono pronunciate frasi mai proferite dai protagonisti. Ingegneria sociale praticata sotto le mentite spoglie della truffa, perpetrata con metodi raffinati, rispetto a cui bisogna rispondere con politiche e strategie di cyber security adeguate. Ha ragione Iezzi nel formulare un invito preciso a tutti gli utenti della Rete. "Bisogna partecipare attivamente alla edificazione di un sistema digitale condiviso. Segnalare contenuti sospetti, sostenere il giornalismo di qualità, e partecipare a iniziative di alfabetizzazione mediatica contribuendo a combattere le manipolazioni e la cultura dell'informazione responsabile". Sottoscrivo queste considerazioni che dovremmo tutti fare nostre.



Verità e falsità: lo spettro dell'uomo di vetro?

Rimanendo sul fronte della* awareness*, esercizio che tutti dovremmo fare. Verità/falsità difficile comprendere dove si colloca il limite tra queste categorie. Ci si può preparare per non cadere nel "tranello"?

Bella domanda! Il problema cominciano a porselo sia gli psicologi che i filosofi, perché nel nuovo contesto diventa sempre più difficile distinguere reale e virtuale, vero e falso, realtà e fantasia. Non ci sono soluzioni, unica cosa che possiamo fare è acquisire coscienza, migliorare la nostra capacità di giudizio critico, migliorare il fronte delle competenze, perché solo la conoscenza può scongiurare le paure.

In conclusione, voglio richiamare un'affermazione del Garante della Privacy Pasquale Stanzione tratta dall'ultima giornata europea della privacy: "Quello che è avvenuto nel campo delle neuroscienze, dove si è realizzato un decoder "semantico" dell'attività neurale a partire dai dati forniti da una risonanza magnetica funzionale, combinando scansione cerebrale e database di modelli linguistici, come quelli usati da ChatGPT, non può non far pensare. Bisogna ricordarsi che la persona non è un archivio liberamente accessibile, altrimenti sarà la condizione dell'"uomo di vetro" a prevalere, senza difese, preda dell'autismo digitale, vittima di una forma atroce di solitudine, vissuta e consumata nello "specchio" deformante della rete. La solitudine digitale è una dimensione dell'esistere con cui dovremo fare i conti?

Si tratta di preoccupazioni del Garante, altamente condivisibili. Temo che non siamo assolutamente lontani da quest'uomo di vetro, considerato come un database pubblicamente accessibile e quindi spogliato della sua riservatezza. Ma del resto, ciò era implicito fin dalla nascita della rete e dalla possibilità che essa offre di raccogliere la "vita" delle persone, dai gusti ai comportamenti, persino all'immaginario, fino ad entrare nel foro che credevamo intangibile della coscienza. ■

La regolazione della società digitale, pilastro della Costituzione europea.

Intervista VIP con Franco Pizzetti.

Autore: Massimiliano Cannata

Professor Pizzetti, comincerei la nostra discussione dal significativo titolo della collana da lei diretta "I diritti nella "rete" della rete". Normare lo sviluppo del digitale è una sfida che La vede impegnata da molti anni, basti pensare l'attività che ha svolto come Presidente dell'Autorità Garante della Privacy. A che punto siamo sul delicato e controverso terreno della regolazione del digitale?

L'Europa sta cercando di fare passi avanti significativi. Il significato del programma della Presidente della Commissione, Ursula von der Leyen sullo spazio unico digitale europeo e sulla rivendicazione digitale dell'UE poggia sui principi della regolazione del digitale. L'UE è un mercato unico, che ha regole omogenee per quanto riguarda l'accesso alle risorse e la prestazione dei servizi. Passando all'epoca digitale ed essendo una gran parte dei servizi necessari a questa società forniti con piattaforme e modalità digitale, occorre definire con nettezza il trattamento dei dati che viene fatto per rendere possibili gli scambi. È fondamentale tutto questo per mantenere il mercato unico, per mantenere, detto in sintesi, una UE che abbia un sistema economico con regole omogenee.

"L'Unione Europea nel definire le norme sul digitale sta di fatto gettando le basi della sua Costituzione. Bisogna comprendere che oggi disciplinare lo sviluppo del digitale vuol dire garantire il funzionamento della società in tutte le sue articolazioni".

Franco Pizzetti, Costituzionalista emerito è da sempre impegnato sulla frontiera "mobile" dello sviluppo scientifico e tecnologico, una frontiera che ha bisogno dell'azione di legislatori illuminati per evolvere nel rispetto dei diritti fondamentali e della trasparenza. In gioco c'è il progresso, parola che vorremmo appartenesse al futuro di tutti i popoli del pianeta finalmente senza discriminazioni. ***"La regolazione europea della società digitale"*** (Ed. Giappichelli) è l'ultimo saggio curato da Pizzetti che raccoglie gli interventi dei giuristi: Simone Calzolaio, Antonio Iannuzzi, Erik Longo e Marco Orofino.

Il potere computazionale e il lavoro del legislatore

Molti studiosi sostengono che l'UE sta esercitando una sorta di* Normative power *in ambito legislativo. Il vecchio Continente vuole fare da guida in questo campo, complesso e decisivo per il futuro?

Non si tratta di fare graduatorie. L'Europa deve andare avanti sul percorso della regolazione della società digitale, in modo che ci sia uniformità e che sia assicurata nel

Continente l'interconnessione tra le reti di trasmissioni di dati. Nello stesso tempo deve essere garantito che i fornitori di servizi digitali che operano nell'Unione o fuori dell'Unione adottino criteri omogenei che consentano a tutti gli operatori economici di continuare a operare nel mercato unico.

Lo sviluppo prepotente della tecno-scienza da un lato ci affascina, dall'altro amplia il perimetro delle vulnerabilità. Come deve muoversi il legislatore in relazione alle dinamiche di un cambiamento profondo che investe tutti, considerato che viviamo: (come Lei ha scritto in un volume celebrativo dedicato ai 25 anni della Privacy): **"In una condizione ibrida, dove linguaggi naturali e artificiali si mescolano, articolando una semantica tutta da decifrare"?**

Come si è mosso quando ha dovuto far coincidere le regole per la circolazione dei pedoni sulle strade con le misure di sicurezza dei veicoli a motore a scoppio. Sono servite nuove regole in materia di infrastrutture che potessero per esempio garantire la sicurezza delle persone. Immaginiamo nel Medio Evo cosa poteva dire attraversare una strada e cosa vuol dire oggi, nell'era della velocità. Un salto quantico è avvenuto, salto che deve trovare una corrispondenza sul terreno delle regole e delle norme di sicurezza. Nella società digitale la dimensione del rischio è ovviamente diversa e bisogna attrezzarsi di conseguenza.

L'importanza di una strategia continentale

Lei ha lavorato molto perché i Garanti europei potessero trovare una reale armonia di intenti. I tempi sono maturi perché più in generale le istituzioni del Continente possano intendersi sulle strategie da seguire?

Credo di sì, perché il mestiere è lo stesso in tutti i paesi. Possono esserci moderate pressioni di un paese rispetto a un altro, ma il cammino è stato

intrapreso. Non dimentichiamoci che regolare l'uso e il trattamento dei dati personali, penso all'epoca che ha visto impegnato una importante figura di giurista come Stefano Rodotà, ha a che fare soprattutto con la sfera dei diritti, oggi normare il digitale vuol dire garantire il funzionamento dell'intera società. Non deve perciò stupirci che a livello europeo ci sia una spinta molto forte a far intervenire la Commissione con poteri di vigilanza in questa materia. Lo si vede molto bene con l'applicazione dell'Intelligence Act, è stato costituito un ufficio per l'intelligenza artificiale presso la Commissione europea con compiti di vigilanza e di sanzione. Il cambiamento sta nel fatto che se le regole hanno una più diretta incidenza sul vivere sociale, non solo e unicamente sui diritti del singolo individuo, l'operatore politico nei sistemi

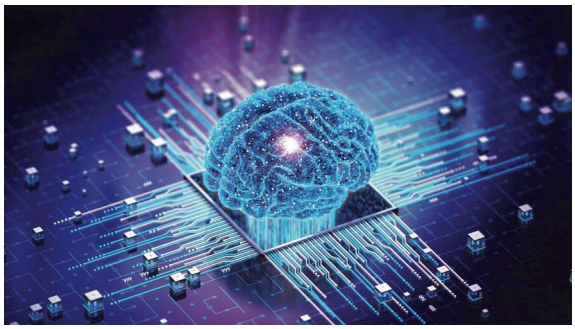
BIO

Franco Pizzetti è professore ordinario di Diritto costituzionale all'Università di Torino; è stato Pro-rettore dell'Università di Torino dal 1984 al 1987 e Vice Rettore dell'Università di Torino fino al 1996; Nel corso della sua carriera ha altresì insegnato: Diritto costituzionale italiano e comparato nell'Università di Urbino, dove è stato docente dal 1973; Diritto regionale nell'Università del Piemonte Orientale; Diritto pubblico e legislazione scolastica nell'Università di Torino. Nel corso della sua carriera ha altresì insegnato: Diritto costituzionale italiano e comparato nell'Università di Urbino, dove è stato docente dal 1973; Diritto regionale nell'Università del Piemonte Orientale; Diritto pubblico e legislazione scolastica nell'Università di Torino. Attualmente è: Presidente di Alleanza per Internet #all4i; Presidente del Working Party on Police and Justice, per la tutela dei dati personali dei cittadini nei settori della giustizia e dell'attività di polizia in ambito europeo (cd. III Pilastro), dal 2007; Presidente della Commissione interministeriale per le intese con le confessioni religiose, dal 1997; Presidente del Comitato Tecnico Scientifico della Associazione Nazionale dei Comuni Italiani (ANCI), dal 2008; Membro del Comitato Tecnico Scientifico della Scuola Superiore della Pubblica Amministrazione Locale (SSPAL), dal 2008.Nel corso della sua carriera è stato altresì: Presidente dell'Autorità Garante per la protezione dei dati personali dal 2005 al 2012; Membro del Consiglio di Presidenza della Giustizia Amministrativa dal 2000 al 2004; Docente stabile di diritto costituzionale – governo locale presso la Scuola Superiore della Pubblica Amministrazione; Direttore della Scuola Superiore della Pubblica Amministrazione; Consigliere giuridico del Ministro della Funzione Pubblica Franco Bassanini dal 1998 al 2001; Consigliere costituzionale del Presidente del Consiglio dei Ministri Romano Prodi dal 1996 al 1998; Vice-Sindaco di Torino dal 1990 al 1993 nella giunta Zanone; Consigliere costituzionale del Presidente del Consiglio dei Ministri Giovanni Goria nel 1987; Segretario della Conferenza Stato-Città Autonomie locali presso la Presidenza del Consiglio dei Ministri. Tra le sue opere si segnalano in particolare: "Rilevanza e non manifesta infondatezza nel giudizio in via incidentale", in collaborazione con G. Zagrebelski (Milano, 1972); "Rigidità e garantismo nella costituzione spagnola" (Casale 1979); "Federalismo, regionalismo e riforma dello Stato" (1° ediz. Torino, 1996 e 2° ediz. Torino 1998); "Il nuovo ordinamento italiano tra riforme amministrative e riforme costituzionali" (Torino, 2001); "L'ordinamento costituzionale italiano tra riforme da attuare e riforme da completare" (Torino 2003); "Privacy e il diritto europeo alla protezione dei dati personali" (Giappichelli 2016).

attuali di democrazia rappresentativa tende a prevaricare le autorità indipendenti di garanzia. Bisognerà trovare un bilanciamento tra queste componenti, cosa che in parte sta già avvenendo. Esiste, inoltre, un incrocio molto preciso tra la tutela dei rapporti che intercorrono tra le persone nella società digitale, e la sfera dei diritti. Diventa perciò cruciale la sopravvivenza, pure in questo nuovo contesto, delle tradizionali autorità di garanzia sia per quanto riguarda i dati personali che per le telecomunicazioni, che più generale per quel che attiene alle libertà di manifestazione del pensiero con modalità digitali.

Si guarda con grande attenzione all'incrocio di cyber spazio e IA. La legge da poco approvata sull'IA, ha generato una sorta di contrapposizione tra "rigoristi" e "liberisti". Si tratta di polemiche sterili?

Evitiamo i facili slogan che riempiono la stampa. Cominciamo a capire cosa è l'IA. Si tratta di una tecnologia che si basa su elevate capacità computazionale e di elaborazione dei dati. Oggi è possibile a costi relativamente contenuti avere accesso a informazioni strategiche per fare analisi dei dati con scopi di carattere previsionale e non solo. Faccio un esempio concreto: se devo organizzare le corse di una metropolitana mi è utile poter analizzare a basso costo il numero di utenti che nelle varie fasce orarie usano il mezzo nelle diverse stazioni della linea perché sulla base di questo posso organizzare un servizio più efficiente e più economico. Questa è sostanzialmente l'IA. È evidente che trattandosi di una tecnologia che comporta l'accesso a un numero molto importante di dati, la loro conservazione e l'accessibilità di questo asset intangibile molto prezioso crea dei problemi.



A cosa si riferisce in particolare?

Al fatto che i dati sono informazioni sulle persone e per questo implicano una tutela giuridica. Bisogna, in particolare, porre una grande attenzione alle imprese, che trattano una grande quantità di informazioni, molte delle quali sensibili. Faccio un esempio per capirci. Se una qualsivoglia istituzione rende accessibile i dati della metropolitana di una città europea a un operatore che vuole partecipare a una gara di appalto come fornitore del servizio, deve attenersi a delle regole che consentano l'utilizzazione delle informazioni. L'IA essendo una tecnologia che ha come habitat la società digitale, che si nutre di una quantità costantemente crescente di dati, che possono essere conservati a costi limitati, come dicevo prima e soprattutto trattati con capacità computazionali molto elevate diventa essa stessa un asset fondamentale del mercato unico europeo. La regolazione dell'IA, al di là del solito fascino del nome, va dunque vista dal puto di vista dell'incidenza che questa tecnologia ha e avrà sull'economia europea. Ancora una volta la sfida è quella di trovare regole per definire forme di intelligenza artificiale omogenee tra tutti i paesi della UE.

La prospettiva del decennio digitale europeo

Questo numero di* Cybersecurity Trends *si occupa della direttiva "NIS2". Molti studiosi si interrogano sugli aspetti applicativi della norma. Quali sono le ragioni di tanto interesse?

Se una società digitale deve operare attraverso il trasferimento e la conservazione dei dati, appare persino ovvio che la sicurezza della rete di trasmissione da un soggetto all'altro è un punto chiave. Il furto di dati è relativo a elementi che possono servire, anche e non solo mediante l'IA, per trarre ulteriori informazioni su alcuni ambiti strategici della società. Appare perciò evidente che la tutela in termini di sicurezza dei servizi che si definiscono ad alto valore aggiunto, crescerà di rilevanza. Non è più, come ricordavo prima una questione che attiene alla riproduzione o contraffazione dei dati personali che rientrano nei profili di tutela di un diritto, siamo di fronte alla necessità di tutelare un sistema sociale.

Gli interventi contenuti del volume convergono nella prospettiva che conduce al "decennio digitale europeo". Ci troveremo di fronte a una nuova ancora poco "leggibile" tappa della rivoluzione digitale?

L'Unione Europea nel regolare i trasferimenti dei dati come pilastro della società digitale sta mettendo, in realtà le basi per la sua COSTITUZIONE. Significa che invece di provvedere prima alla stesura della costituzione per poi definire le regole per attuarne il contenuto costituzionale si sta operando in senso inverso. In merito al decennio digitale è possibile che la prossima Commissione lo prolunghi, magari inventando nuove fascinose etichette; in sostanza, va detto che con la regolazione della società digitale si è iniziato un cammino che condurrà velocemente verso la Costituzione europea. Questo non deve stupirci dal momento che la società è radicalmente cambiata sulla spinta delle trasformazioni tecnologiche, ne discende che la formula di riconoscimento dei diritti fondamentali deve necessariamente avere una rilevanza costituzionale. ■

Security Mind

La Cyber Security incontra La Psicologia

A cura di Veronica Patron Co-Founder di Security Mind

Dalla Direttiva al Comportamento: NIS 2 e Psicologia nell'Era Digitale

Nel campo della sicurezza informatica, l'adozione della Direttiva NIS 2 (Network and Information Systems Security Directive 2) rappresenta un passo avanti nell'approccio dell'Unione Europea alla resilienza delle infrastrutture critiche.

Per realizzare i suoi obiettivi la NIS2 ha previsto una serie di azioni tra cui la formazione e sensibilizzazione dei dipendenti sui protocolli ottimali di sicurezza informatica.

La sicurezza informatica oltre ad essere una questione di tecnologia, è anche influenzata dal comportamento umano.

Psicologia Comportamentale e Sicurezza Informatica con la NIS 2

Il comportamento umano è spesso il fattore più imprevedibile nei sistemi di sicurezza informatica. Gli errori umani possono variare dall'utilizzo di password deboli e facilmente indovinabili, al cliccare su link dannosi, ritardo negli aggiornamenti dei software di sicurezza.

Questi comportamenti possono essere influenzati da una vasta gamma di fattori psicologici:

ECCESSO DI FIDUCIA
Alcune persone sopravvalutano la loro capacità di riconoscere ed evitare le minacce online, portandole così a prendere decisioni meno prudenti.

STANCHEZZA E STRSS
La fatica può ridurre l'efficacia del giudizio di una persona e la capacità di seguire le migliori pratiche di sicurezza, rendendo gli errori più probabili.

ABITUDINI
Le persone tendono a preferire soluzioni che minimizzino lo sforzo, anche se in alcuni casi può compromettere la sicurezza.

L'importanza di una formazione innovativa nella prevenzione degli attacchi informatici

Gli attacchi sfruttano le debolezze umane per indurre le vittime a rivelare informazioni confidenziali o a eseguire azioni che compromettano la sicurezza.
E' quindi essenziale una formazione oltre che tecnica anche psicologica, formare i dipendenti a gestire le emozioni che gli attacchi di ingegneria sociale cercano di sfruttare, come l'urgenza o la paura, con l'obbiettivo di ridurre la probabilità di successo di tali attacchi.

Incorporando la comprensione psicologica nella formazione sulla sicurezza informatica, le organizzazioni possono sviluppare difese più robuste contro le tattiche di manipolazione, proteggendo meglio le loro infrastrutture e i dati sensibili.

La nostra Missone è passare dall' Informazione alla Trasformazione

www.securitymind.cloud

Roberto Mania
Capitalisti silenziosi
Egea Ed.

Autore: Massimiliano Cannata

Le imprese familiari con le carte in regola per guidare la ripresa

"Avevamo l'America in casa e non ce ne siamo accorti" scrive Roberto Mania nel saggio inchiesta "Capitalisti silenziosi" (ed. Egea) in cui racconta la rivincita dell'impresa familiare, sfatando tanti luoghi comuni. Abbiamo per troppo tempo collocato le famiglie imprenditoriali nel recinto di un conservatorismo miope, impegnate solo a difendere l'esistente e la ricchezza acquisita. Quella convinzione va rivista, sostiene l'autore, perché questo modello è stato il vero baluardo che ha saputo reggere alla crisi della globalizzazione. Voce importante non solo in termini di PIL, queste aziende hanno espresso un patrimonio di know-how, saperi condivisi e buone pratiche, coniugando eccellenza e talento. Il "doppio legame" tra etica ed economia, l'attenzione per l'"eco-sistema" oltre che l'amore per la propria terra sono fattori distintivi di un modo di concepire il business che parte dal rispetto per la coscienza e l'identità dei luoghi, creando legami. I numeri aiutano a capire: a livello internazionale, l'Italia si colloca al settimo posto tra i Paesi che ospitano le prime 500 società familiari al mondo; circa l'80% per cento delle PMI hanno una matrice familiare, sono ben distribuite nella fascia delle medie (57 per cento), ma anche molto presenti nel comparto delle grandi (35,6 per cento) con un valore complessivo di fatturato che supera i 900 miliardi di euro. Importante opera di ammortizzatore sociale hanno svolto questi imprenditori, concorrendo alla creazione dell'occupazione (+20,1 per cento in sei anni) anche nel momento terribile della pandemia. Tra le prime 100 aziende più antiche al mondo, 15 sono italiane e tra queste, se ne contano 5 che risultano tra le 10 aziende familiari più antiche tuttora in esercizio. Mentre il mondo militarizza e chiude i confini, atterrito dalle guerre, le famiglie imprenditoriali hanno reagito conquistando clienti e mercati, innovando la catena del valore, facendo da motore ai nuovi "distretti". Il racconto di Mania non è una voce isolata. Molti studiosi e uomini d'impresa stanno guardando con interesse alla riemersione di questo paradigma. "Orientamento al cliente e flessibilità nell'approccio imprenditoriale sono state le componenti di successo – commenta Pier Luigi Verbo, responsabile public sector KPMG – che vanno misurate in relazione alla spiccata attitudine al sacrificio, cultura del lavoro, ascolto degli *stakeholder*, senso di responsabilità. Individualismo e senso civico hanno costituito quel mix virtuoso, che connota l'identikit di una classe di imprenditori che si è emancipata da vecchi retaggi e dalle influenze della politica e oggi appare desiderosa di affrontare il mare aperto della competizione senza sperare in "aiutini" di Stato. L'impegno per la difesa assoluta di saperi esclusivi, abilità "artigiane", originalità dei *know how*, è stata ed è una importante carta vincente, che spiega il successo di tante storie del nostro *made in Italy*, che non dimentichiamolo mai, nascono e crescono in ambito familiare. Oggi la sfida della transizione tecnologica e della sicurezza sono ulteriori parametri che sollecitano le nostre imprese a essere all'altezza. Il cambiamento d'epoca sta facendo saltare le gerarchie, non sono, infatti, solo i grandi nomi a occupare la scena mediatica. Uomini capaci, con silenziosa concretezza stanno avendo la loro rivalsa. Questa nuova classe dirigente manageriale – spiega Roberto Panzarani – possiede una nuova connotazione la *Humbition*, destinata a caratterizzare la classe dirigente del futuro. Si tratta di un mix di umiltà e ambizione, che si traduce in una sostenibile prontezza nel riconoscere i propri errori, disponibilità a usare le conoscenze per connettersi ai collaboratori. È evidente che da una *governance* le aziende potranno trarre vantaggi crescenti.

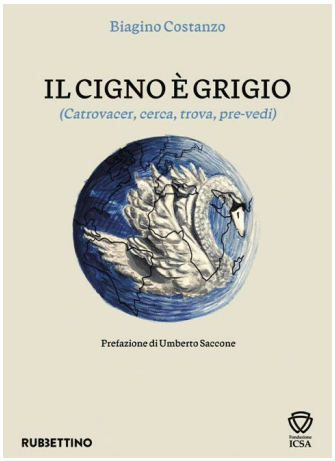
Inoltre, va detto che l'esercizio di queste virtù sarà decisivo per competere sui sentieri dell'internazionalizzazione, innescare le leve del ricambio generazionale, gettando le basi per la costruzione di una borghesia produttiva che potrà contribuire, in maniera incisiva, al rilancio del made in Italy riaffermando l'identità del nostro Paese nella complessa trama della contemporaneità. ■

Biagino Costanzo
Il cigno è grigio
Rubbettino ed.

Autore: Massimiliano Cannata

Torniamo ad esercitare il "pensiero lungo" per sconfiggere le crisi permanenti

Offre interessanti spunti per una lettura trasversale *Il cigno è grigio*, saggio di Biagino Costanzo. Manager con un'esperienza trentennale, già consulente della presidenza del Consiglio, docente di scienze forensi e criminologiche, socio della Fondazione ICSA. Lo studio si può considerare la naturale prosecuzione di un precedente lavoro di ricerca "Saligia" (Bastogi editore, n.d.r.) focalizzato sugli "inciampi dell'evoluzione". Perché sono le battute d'arresto, le bibliche "pietre d'inciampo" che appassionano lo studioso e che obbligano tutti noi a riflettere, andando oltre gli stereotipi e il



pensiero dominante. "Saligia – spiega l'autore - è l'acronimo dei sette vizi capitali che viene utilizzato per fotografare il decennio 2007-2017 dove la società ha iniziato a "sbandare", non avendo più punti di riferimento certi. Tutto è iniziato con la fine delle ideologie e con la globalizzazione buona che si è trasformata in un capitalismo esclusivamente finanziario. Il cambiamento in peggio dal punto di vista antropologico già era in nuce. Oggi viviamo in una bolla del nulla e del superficiale dove, anche dal punto di vista professionale, molti tentano di aggiustare il tiro, operazione alquanto difficile da attuare".

Siamo oltre la società del rischio di Ulrich Beck. Gli sconvolgimenti cui siamo sottoposti hanno scompaginato le categorie di riferimento esistenziali, ontologiche e conoscitive. La prepotente espansione del cyber crimine è un'autentica emergenza del nostro tempo, che richiede investimenti in capitale umano e strumenti. Rispetto a questi temi, già prioritari nelle agende dei governi, Costanzo, come evidenzia molto bene Umberto Saccone nella prefazione, mostra "un evidente, consolidato, autentico e convinto rifiuto dell'ipocrisia". L'incessante progresso e i rapidi cambiamenti innalzano in modo esponenziale la percezione del pericolo, dovuto innanzitutto all'aumento della popolazione mondiale, fattore che ha determinato una richiesta sempre più massiva di sicurezza. I rischi per la privacy sono diretta conseguenza di un mutamento del quadro, con cui dovremo imparare a fare i conti".

"Permacrisi" è l'originale neologismo che attraversa le pagine. Si tratta, come viene spiegato nei dizionari, di una condizione di crisi permanente, per cui si passa da un'emergenza all'altra. "Solo 15 anni fa abbiamo fronteggiato la peggiore crisi finanziaria dagli anni '30, poi la peggiore pandemia dal 1919 e ora la più grave crisi-geopolitica in Europa dalla fine della guerra fredda in uno con le tensioni mediorientali che possono destabilizzare l'intero mediterraneo. Pandemia, cambiamenti climatici, guerra con minaccia nucleare, razionamento energetico, inflazione. Viviamo una nuova normalità dove l'ansia costante pervade, senza soluzione di continuità, le nostre vite". È in questo particolare clima che scopriamo le fattezze inedite del "cigno grigio", quando avevamo sempre creduto che fosse nero. Vale la pena seguire il ragionamento dello studioso: "Quella del cigno nero è una teoria scientifica che descrive un evento non previsto, che ha effetti rilevanti e che, a posteriori, viene razionalizzato e giudicato prevedibile. Etimologicamente questa teoria prende le mosse dall'errata assunzione nell'emisfero boreale dell'inesistenza del cigno nero, "scoperto" dal mondo occidentale, solo nel 1697. In realtà, come cerca di dimostrare nel suo scritto, quasi tutto è prevedibile, si può dunque abbassare il livello del rischio, mettendo in campo azioni efficaci. Cosa c'è di nero ed imprevedibile in una carestia, in una migrazione di massa, agevolate dal cambiamento climatico? Cosa c'è di nero ed imprevedibile circa la possibilità che si possa verificare un incidente nucleare ad una delle tante centrali nucleari disseminate nel mondo? Cosa c'è di nero ed imprevedibile in una crisi energetica aggravata da una non imprevedibile guerra che ha portato alla luce politiche di approvvigionamento dell'energia poco lungimiranti? Cosa c'è di nero ed imprevedibile in una inondazione di fake news e di una narrazione falsa di fatti ed avvenimenti? L'IA se non governata eticamente e con serietà dove ci porterà?".

Sono tutti interrogativi pesanti quelli sollevati dal testo che spingono il corpo collettivo a ritornare a esercitare un "pensiero lungo". Ridare spazio al ragionamento, alla riflessione, superando il "pensiero breve", può essere una ricetta utile per pensare positivo senza sfociare nell'utopia. Il "cigno grigio" è una provocazione che può aiutarci a mutare atteggiamento e a rileggere il percorso dell'evoluzione con rigore scientifico, evitando di cadere nei facili slogan e nelle tante illusioni ottiche che distraggono l'"opinione pubblica dalle questioni reali che dovremo affrontare per ridare fiato alla crescita e imboccare un percorso credibile per lo sviluppo umano. ■

XIX Rapporto Censis sulla comunicazione Ed. Franco Angeli

Autore: Massimiliano Cannata

Il vero e il falso nella società di Internet

Nel 19° Rapporto sulla Comunicazione del Censis emerge un fenomeno che preoccupa più di due terzi della popolazione: il disfacimento delle categorie del vero e del falso, cancellate dalla prepotente diffusione dell'IA. Mentre non si ferma il boom della spesa delle famiglie per i dispositivi digitali (8,7 miliardi di euro aumento del 700% dal 2007) e i motori di ricerca, in particolare YouTube la fanno da padroni, la "dieta" mediatica degli italiani appare fortemente condizionata da questa nuova consapevolezza. Si avverte un bisogno crescente di qualità e di indipendenza dell'informazione. La tecnologia sta modificando la produzione e la confezione delle notizie, l'intelligenza generativa è entrata nelle redazioni, assumendo sembianze ancora difficili da definire. Il caso di Google che paga degli editori per addestrare i propri dispositivi per imparare a scrivere articoli autonomamente è un

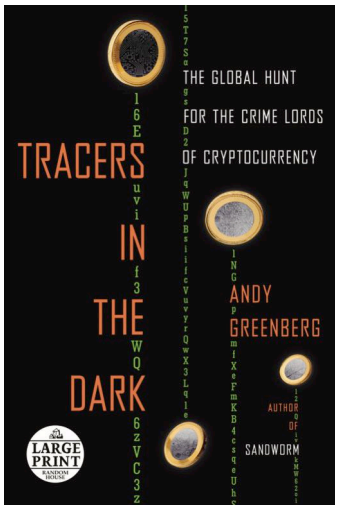
segno dei tempi. La macchina dell'informazione sta modificando le sue logiche produttive, questo crea disorientamento non solo tra gli addetti ai lavori, ma più in generale nell'opinione pubblica. Le *Fake news* dominano l'orizzonte, creando "pezzi" di verità, allo scopo di indirizzare non solo i flussi elettorali e le elezioni, ma persino scelte economiche e geopolitiche che hanno un peso strategico sul futuro del Pianeta. La gravità del fenomeno è comprovata dal primo report che il teologo e consulente di papa Francesco, Paolo Benanti ha redatto per l'esecutivo, denunciando i pericoli per la democrazia, legati al rapporto promiscuo di verità e falsità, tratto distintivo dell'ecosistema digitale che permea società, istituzioni e imprese. Esiste un problema di credibilità e affidabilità, che il comportamento degli utenti non nasconde. Nell'ultimo anno si è mantenuto stabile il livello di credibilità del media più *mainstream*, la TV. Sorprende la tenuta della cara vecchia radio, anche se l'approvvigionamento delle notizie, soprattutto nella fascia che va di 14 ai 30 anni si è spostata sui dispositivi mobili. Una migrazione che risponde alla velocità, cifra connotante di Internet. Non a caso Instagram si impone come *"l'enfant prodige"* dei social considerato dal 15% degli utenti una fonte di informazione a tutti i livelli. In questo scenario, che sembra consolidare un trend antropologico netto, si stanno però facendo strada nuovi atteggiamenti. Il popolo degli internauti, ormai stordito dalla volatile superficialità che invade i siti di notizie senza fondamento, si rivolge con interesse all'informazione di qualità, che per il 74% del campione interpellato è giusto che non sia gratis. Per questo devono avere spazio gli esperti, che possono aiutare l'ascoltatore e il lettore a interpretare la trama della complessità del mondo oggi. Torna fortunatamente a imporsi, in questa affannosa ricerca di affidabilità, il ruolo dei giornalisti che, come prevede l'etica della professione, devono verificare e confrontare con filtro critico le fonti per offrire materia di giudizio indipendente a un corpo collettivo, spesso disorientato e non sempre adeguatamente attrezzato per capire i retroscena legati a fatti ed eventi. Non dimentichiamoci che una società che non trova spazio per la verifica delle fonti rischia di rimanere preda delle false narrazioni. "La speranza – commenta Luciano Floridi – è che l'IA piuttosto che uno specchio deformante della nostra esistenza, ci renda inquieti, ancora desiderosi di lottare per la verità, che impone una ricerca aperta che non ha mai fine". ■

Andy Greenberg Tracers in the dark Randome House ed.

Autore: Massimiliano Cannata

Un thriller affascinante ci fa scoprire i lati oscuri del web

"Tracers in the Dark" di Andy Greenberg è un'avvincente narrazione che ci trasporta nel cuore dei mercati neri digitali, illuminando i recessi una volta oscuri e apparentemente inaccessibili



del mondo della criptovaluta, in particolare del Bitcoin. Con una prosa coinvolgente, Greenberg ci introduce a una nuova generazione di investigatori, dotati di una combinazione letale di abilità tecniche, forensi, finanziarie e pura determinazione, che hanno scoperchiato il velo di anonimato che avvolgeva i territori del denaro, delle droghe e della violenza sul web.

Attraverso un'analisi accurata e appassionante, l'autore ci conduce attraverso un labirinto digitale di crimine e inseguimenti, popolato da agenti federali, imprenditori danesi e una gamma variegata di personaggi dal passato turbolento. Con una padronanza senza pari della materia, Greenberg ci racconta una saga sorprendente di imperi criminali eretti e distrutti nel mondo oscuro della cripto-economia. Una storia cruciale su Internet, il dark web e la polizia nell'era digitale, la ha definita Cyberscoop. Il libro dimostra con dettagli avvincenti e talvolta emozionanti come le forze dell'ordine, come l'unità investigativa criminale dell'IRS, abbiano sfruttato la potente tecnologia emergente per rintracciare la criptovaluta, che una volta sembrava anonima, direttamente alle porte di alcuni dei criminali più ricercati al mondo... Un mondo quello delle criptovalute tutto ancora da scoprire. Greenberg aiuta il lettore a creare un suo percorso conoscitivo, delineando l'evoluzione di una disciplina completamente nuova. Dettagli tecnici e costruzione di una semantica adatta a entrare nei meandri del web danno corpo a un metodo originale per parlare di cyber security.

"Tracers in the Dark" è, infatti, molto più di un semplice racconto di azione e avventura. È una riflessione profonda sulle dinamiche del potere e sulle implicazioni etiche e sociali di una tecnologia apparentemente neutrale come la blockchain. L'autore solleva interrogativi provocatori sul comportamento dei criminali più audaci, se fossero convinti di rimanere al riparo dalle conseguenze delle proprie azioni. La tessitura del racconto è mirabile e ne fa un capolavoro di reportage investigativo che non solo cattura l'immaginazione del lettore, ma lo spinge a riflettere sulla complessità e le sfide della società digitale contemporanea. L'intreccio tra componente tecnologica, studio della criminalità, e pratica della giustizia è un ulteriore aspetto che fa riflettere. Indagare gli angoli oscuri del cyber spazio non è un esercizio arduo per addetti ai lavori, ma un "pezzo" della vita reale con cui dobbiamo imparare a fare i conti. Il messaggio di Greenberg è molto chiaro, bisogna saper disporre la mente e il cuore ad accoglierlo. ■

Guida per la protezione dei bambini nell'uso di internet

Proteggere i bambini on-line è una sfida globale che richiede un approccio globale. Mentre molti sforzi per migliorare la protezione online dei bambini sono già in corso, la loro portata finora è stata più di carattere nazionale che globale. L'ITU (Unione Internazionale delle Telecomunicazioni) ha avviato l'iniziativa Child Online Protection (COP) per creare una rete di collaborazione internazionale e promuovere la sicurezza online dei bambini in tutto il mondo. COP è stato presentato al Consiglio ITU nel 2008 e approvato dal Segretario generale dell'ONU e da capi di Stato, Ministri e capi di organizzazioni internazionali provenienti da tutto il mondo.

Poste Italiane, insieme alla propria Fondazione GCSEC e alla Polizia Postale e delle Comunicazioni ha prodotto la Versione italiana delle linee guida ITU, guida per la protezione dei bambini nell'uso di Internet e guida per genitori, Tutori ed insegnanti per la protezione dei bambini nell'uso di Internet.

Linee guida per genitori, tutori ed educatori per la protezione on line dei bambini

Seconda Edizione, 2016

www.itu.int/cop

Una pubblicazione

web for business
swiss webacademy

Redazione:

Laurent Chrzanovski e Romulus Maier (†)

(tutte le edizioni)

Per l'edizione italiana:

Nicola Sotira, Elena Agresti

ISSN 2559 - 1797

ISSN-L 2559 - 1797

Indirizzi:

info@cybertrends.it

Şcoala de Înot nr.18, 550005,

Sibiu, Romania

www.swissacademy.eu

www.cybertrends.it

CYBERSECURITY TRENDS

SOSTIENI IL GIORNALISMO INDIPENDENTE

DONA ORA

Il tuo contributo è prezioso 💎
www.cybertrends.it/donate/