CYBER MAGAZINE

CYBER Think Tank ASSINTEL

ASSINTEL
ASSOCIAZIONE NAZIONALE IMPRESE ICT

Giugno 2024

Intervista Speciale ◆ Intervista Speciale ◆ Intervista Speciale

Intervista Speciale ◆ Intervista Speciale ◆ Intervista Speciale

Cyber Think Tank Assintel

CYBER
Think Tank
ASSINTEL

La conoscenza è la nostra arma migliore.

Unisciti a noi al prossimo meeting del Cyber Think Tank!

Prossimo Incontro

10 Luglio

14:00 - 15:30

CYBER THINK TANK ASSINTEL

INDICE

ESCLUSIVA

Intervista al sindaco di Milano Giuseppe Sala

Pg. **10**

ESCLUSIVA

Intervista Speciale

A colloquio con Pasquale Stanzione:
serve una pedagogia digitale per arrestare la violenza in Rete e ridare sostanza alle promesse

Di Massimiliano Cannata

Pg. **12**

Garantire la sicurezza degli oggetti grazie all'Identity of Things

Di Danilo Cattaneo

Pg. **16**

La cyber security al centro - i paradigmi dell'industria di oggi e domani

Di Marco Comastri

Pg. **18**

AI Act: il Regolamento europeo in materia di Intelligenza Artificiale

Di Ranieri Razzante

Pg. **20**

Costruire Ponti Digitali: l'interoperabilità nella lotta contro le minacce informatiche

Di Sandra Marsico

Pg. **22**

Alfabetizzazione Cyber: l'approccio del Cyber Think Tank Assintel

Di Carlo Guastone Pg. **26**

Neuroscienze, guerre cognitive e narrazioni digitali

Di Marco La Rosa Pg. **28**

Direttiva NIS2 (e direttiva CER) opportunità per le imprese, solo se gestita bene

Di Alessandro Manfredini Pg. **30**

Menti sotto assedio: la rivoluzione umana nella cybersecurity

Di Petra Chiste Pg. **32**

Cybersecurity: necessario innovare davvero prima che diventi il tallone d'Achille dell'Italia

Di Pierluigi Paganini Pg. **36**

L'utilizzo dell'IA nella cybersecurity

Di Paolo Montali Pg. **38**

Il brand "Made in Italy" nel settore agroalimentare: un volano per l'economia italiana

Di Marco Porcedda Pg. **41**

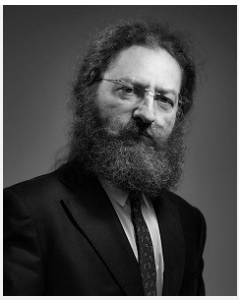
Il cert finanziario italiano (CERTFin): rafforzare la cyber resilience di settore attraverso la cooperazione pubblico-privata

Di Mario Trinchera Pg. **44**

Data breach regione Lazio

Di Paola Righetti Pg. **46**

Minacce 2030



Di Corrado Giustozzi Pg. **48**

L'evoluzione del ruolo della sicurezza cibernetica con l'avvento delle più recenti tecnologie di frontiera

Di Paolo Dal Cin Pg. **50**

Multi-Factor Authentication: è davvero una panacea?

Di Enrico Morisi Pg. **52**

L'importanza strategica delle analisi di Threat Intelligence nella gestione della Supply Chain

Di Martina Fonzo Pg. **54**

AI – Domande e risposte facili facili: l'AI per la scienza e la medicina

Di Gianpiero Cozzolino Pg. **56**

L'Attribute Based Encryption per sfruttare al meglio i dati e ridurre il rischio di compromissione

Di Dolman Aradori Pg. **58**

I nuovi Trend dello scenario cybercriminale

Di Sofia Scozzari Pg. **60**

WEBINAR

AI ACT & DDL AI Italia:

obblighi adempimenti e rischi per le aziende

Relatori:

Pierguido Iezzi

Enzo Veiluva

Alessia Valentini

CYBER Think Tank ASSINTEL

28 giugno

12:00 - 13:00

Per info scrivi a:

segreteria@assintel.it

L’editoriale del Coordinatore del Cyber Think Tank Assintel Pierguido Iezzi

Giugno 2024

Carissimi lettori,

È con immenso piacere che vi presentiamo il quinto numero del Cyber Magazine di Assintel, una pubblicazione che continua a crescere e a evolversi grazie al contributo di esperti del settore e alla vostra costante partecipazione. Questo numero è particolarmente speciale poiché ospita un’intervista esclusiva con il Sindaco di Milano, Giuseppe Sala, che ci offre una visione unica sul ruolo della tecnologia e della cybersecurity nel futuro della nostra città. Il panorama della cybersecurity è in costante evoluzione, e in questo numero esploriamo temi di cruciale importanza, dalle neuroscienze alle guerre cognitive e narrazioni digitali. Scoprirete come l’IA stia rivoluzionando la scienza e la medicina, e l’importanza strategica delle analisi di Threat Intelligence nella gestione della Supply Chain. Affronteremo anche argomenti di stretta attualità come la Direttiva NIS2, le opportunità e le sfide che essa presenta per le imprese, e discuteremo dell’AI Act, il nuovo regolamento europeo in materia di Intelligenza Artificiale. Non mancheranno riflessioni sulla necessità di una pedagogia digitale per combattere la violenza in rete e sul ruolo della Multi-Factor Authentication nella protezione dei nostri dati. Vi invitiamo a immergervi in questi articoli, ricchi di approfondimenti e spunti di riflessione, che mirano a fornire una panoramica completa e aggiornata delle sfide e delle opportunità nel mondo della cybersecurity. Un ringraziamento particolare va ai nostri autori e collaboratori per il loro prezioso contributo e a voi, cari lettori, per il vostro continuo supporto e interesse. Vi auguriamo una lettura stimolante e proficua!

Pierguido Iezzi

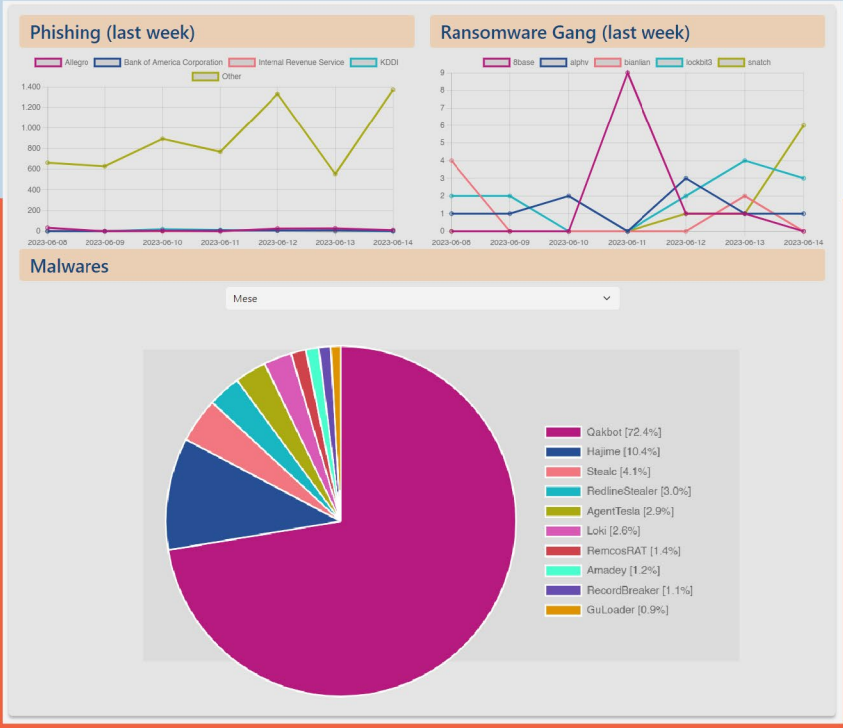
CYBER Think Tank ASSINTEL

Cyber Think Tank Assintel

CYBER Think Tank ASSINTEL

Threat Infosharing

Garantire agli Associati Assintel un servizio di early warning sulle minacce e rischi cyber giornalieri.



Per info scrivi a: segreteria@assintel.it

Intervista al Sindaco di Milano

Il Sindaco Giuseppe Sala

Qual è il suo parere sull'importanza di coinvolgere attivamente i cittadini nella sicurezza digitale del Comune?

Garantire la sicurezza digitale e la protezione dei dati sensibili di cittadini, cittadine e imprese che dialogano con il Comune attraverso sportelli e piattaforme virtuali è fondamentale per Milano, una città considerata "smart", contemporanea, al passo con i tempi e attenta alle novità del mondo digital. Di lavoro ce n'è ancora molto da fare, ma siamo soddisfatti dei risultati raggiunti finora nel campo della trasformazione digitale, anche sul fronte sicurezza. A gennaio 2024, ad esempio, abbiamo attivato il sistema di autenticazione a due fattori, per garantire maggiore protezione dei dati personali e un accesso più sicuro per gli utenti dei servizi online messi a disposizione dall'Amministrazione.

La digitalizzazione è un elemento chiave del progresso e della modernizzazione delle città. Quali iniziative il Comune di Milano sta adottando per promuovere la digitalizzazione e come queste si integrano con la sicurezza digitale?

Come abbiamo detto, Milano è una città leader nel campo dell'innovazione e della digitalizzazione, tanto da ottenere il riconoscimento di "CittàDigitale2023", secondo gli indici di ICity Rank. Fruizione dei servizi online, accesso alle piattaforme nazionali tramite Spid e Cie, transazioni PagoPa, accessibilità e sicurezza del portale, canali di interazione con la cittadinanza, wi-fi pubblico, cablatura sono alcuni degli elementi alla base della transizione digitale di Milano. Una transizione cui vengono accompagnati i cittadini di ogni età anche attraverso programmi di formazione, come il progetto Cybersecurecity.it, promosso dal Comune con Fondazione Assolombarda. Tra i corsi non mancano quelli con focus specifico sulla sicurezza digitale e i pericoli o le truffe di cui si può rimanere vittima sulla Rete, fondamentali per una navigazione consapevole e in sicurezza.

Alla luce del Piano Nazionale di Ripresa e Resilienza (PNRR), quali sono i progetti specifici che il Comune di Milano ha pianificato o sta implementando per potenziare la sicurezza digitale e sfruttare le opportunità di digitalizzazione?

Il Comune di Milano ha già ottenuto il finanziamento

PNRR per una decina di interventi per la trasformazione digitale, per un valore di circa 18 milioni di euro. Si tratta di progetti e iniziative che mirano a rendere più versatili ed efficienti i servizi offerti dal Comune, sostenendo e accelerando allo stesso tempo il processo di transizione al digitale della città. Tra questi interventi, abbiamo la migrazione su cloud, i servizi dedicati alla cittadinanza digitale, l'adozione dell'app IO e della piattaforma PagoPA, l'estensione dell'uso delle piattaforme nazionali di identità digitale (Spid e Cie) e dell'anagrafe digitale. Inoltre, sono finanziati il progetto MaaS4Italy (Mobility as a service) e Living Lab, la piattaforma di notifiche digitale, oltre a progetti dedicati ai servizi di cybersicurezza e di interoperabilità dei dati.

Gli investimenti in sicurezza digitale possono richiedere risorse significative. Come il Comune di Milano intende affrontare la questione dei finanziamenti per garantire un adeguato livello di sicurezza digitale, soprattutto considerando le sfide e le opportunità presentate dal PNRR?

I fondi PNRR al momento destinati alla trasformazione digitale di Milano sono circa 18 milioni di euro, una somma che sarà utilizzata anche per la sicurezza digitale, ma non in via esclusiva. Se sono sufficienti? Certamente no: occorrono ulteriori risorse sul capitolo specifico, per sviluppare gli strumenti digitali indispensabili per permettere ai cittadini di accedere ai servizi in piena sicurezza. Questo però ci sfida a impegnarci per reperire i finanziamenti necessari a raggiungere i livelli di cybersicurezza che una città come Milano, con 1,4 milioni di abitanti e altrettanti city users – con il flusso delle relative interazioni digitali che ne deriva - merita.

Considerando l'iniziativa del Cyber Think Tank Assintel e la recente creazione della piattaforma Cyber Threat Infosharing, come pensa che questa possa contribuire alla sicurezza digitale del Comune di Milano e delle sue aziende?

Mettere a disposizione di imprese e cittadini informazioni utili a identificare le minacce informatiche, per prevenirle o a reagire in maniera corretta, come prevede la piattaforma Cyber Threat Infosharing, è fondamentale per garantire la sicurezza digitale generale della comunità in cui viviamo. Ancora una volta, la collaborazione tra pubblico e privato risulta strategica, perché la condivisione di esperienze, conoscenze e competenze - tecniche e tecnologiche - è indispensabile per migliorare le performance in un ambito tanto delicato come la cybersicurezza, su cui non si possono ammettere deroghe.

"Ancora una volta, la collaborazione tra pubblico e privato risulta strategica, perché la condivisione di esperienze, conoscenze e competenze - tecniche e tecnologiche - è indispensabile per migliorare le performance in un ambito tanto delicato come la cybersicurezza, su cui non si possono ammettere deroghe."

Serve una pedagogia digitale per arrestare la violenza in rete e ridare sostanza alle promesse di libertà e democrazia

A colloquio con Pasquale Stanzione, ***Presidente Autorità Garante per la protezione dei dati personali***

A cura di Massimiliano Cannata

Ogni anno la Giornata dedicata al diritto alla protezione dei dati personali voluta dal Consiglio d'Europa rappresenta l'occasione per riflettere sulle implicazioni sociali ed economiche dell'innovazione tecnologica. Pasquale Stanzione, presidente dell'Autorità ha scelto di soffermarsi sulle fenomenologie della violenza, che trovano nella Rete uno specchio riflettente di preoccupante amplificazione, come fa vedere molto bene la cronaca ogni giorno.

Presidente Stanzione, il focus della sua approfondita e intensa relazione è individuabile in un binomio molto preciso: la violenza della rete e nella rete. Non certo una duplice dimensione che deve far riflettere. Quali scenari si stanno aprendo su questo delicato fronte?

Le interrelazioni tra il web e la violenza sono più profonde e ambivalenti di quanto la drammatica contabilità delle loro aberrazioni può far pensare. Siamo di fronte a uno degli aspetti che Natalino Irti definisce "irresistibile normatività della tecnica", a proposito della sua particolare attitudine a modificare struttura, relazioni, dinamiche e culture, incidendo nel profondo nell'antropologia sociale. La rete, esprime, infatti, la morfologia sociale dell'oggi. La sua degenerazione non può non intrecciarsi con la drammaticità dei problemi epocali, a partire dagli episodi sempre più frequenti di diffusione sui social di immagini di stupri commessi da ragazzi, in gruppo, su ragazze, sole. Eventi drammatici che non possono essere sottovalutati.

Sotto scacco le garanzie di pluralismo informativo e politico

Molteplicità ed efferatezza delle forme di violenza allarmano l'opinione pubblica. Possiamo prenderne alcune in esame?

Prenderei come primo esempio, una forma sottile e ambigua di violenza intesa come condizionamento delle scelte, non solo di consumo ma anche politiche come insegna il caso Cambridge Analytica. Attraverso il pedinamento digitale e la conseguente profilazione della persona si tende a modellare, infatti, il messaggio commerciale, informativo o finanche politico da promuovere e la rappresentazione del reale che si ritiene più utile rendere, orientando il consenso verso il risultato voluto. Si eludono così, in una sorta di brain-hacking, le garanzie del pluralismo informativo e politico, nonché dell'autodeterminazione del cittadino, con il rischio di una manipolazione del consenso tale da alterare profondamente i più importanti processi democratici.

In che misura i fenomeni di cui stiamo parlando incidono sulla libertà della persona?

Con diversa modalità e intensità. Il nudging, tipica forma di manifestazione del potere privato delle piattaforme, per quanto condizioni l'esercizio di alcuni fondamentali diritti, anche politici, non può essere paragonato all' efferatezza di immagini di abusi sessuali diffuse in rete, con la loro carica ulteriormente lesiva per la vittima, che si spinge fino all'umiliazione indotta dall' hate speech. Sono per altro diversi gli autori e le dinamiche di queste violazioni: nel primo esempio preso in esame sono le

piattaforme stesse, negli altri casi sono gli utenti che si avvalgono dello strumento digitale per vessare, umiliare, discriminare gli altri o anche "solo" amplificare, sfruttando la potenza di fuoco del web, gli effetti di abusi consumati nella dimensione reale.

Siamo dentro il "lato oscuro" del web, di cui ancora poco si conosce. Quali sono i rischi da cui dobbiamo tutelarci?

Il "lato oscuro" della Rete si presta a delle logiche di sopraffazione che finiscono con il contraddirne l'originaria promessa democratica. La rete si può oggi presentare come spazio deviante, canale e mezzo di realizzazione di reati, in primo luogo contro interessi collettivi primari. Significativo, in questo senso, il cybercrime o, comunque, l'uso della rete a fini istigativi, propagandistici, reclutativi, apologetici del terrorismo. Si sta per altro registrando, un significativo aumento (imputabile anche al parallelo maggiore ricorso all'e-commerce) anche delle attività predatorie on-line, che hanno determinato, secondo i dati della Polizia postale, il deferimento all'autorità giudiziaria di 3.500 persone nell'anno. Sono le caratteristiche stesse del mezzo digitale che incidono profondamente sulla dinamica della violenza che lì si manifesta: persistenza, pervasività, emulazione, difficile contendibilità. Una volta immessi in rete i contenuti vi restano tendenzialmente per sempre: se ne perde la signoria, vengono condivisi da utenti terzi, diventa perciò difficile rintracciarli nella catena infinita di link in cui spesso finiscono. È inevitabile che il fitto intreccio di queste fenomenologie incidono sulla percezione di sicurezza degli utenti che sentono la legittima esigenza di frequentare la rete come strumento di lavoro e di acquisizione della conoscenza.

Il "lato oscuro" della Rete si presta a delle logiche di sopraffazione che finiscono con il contraddirne l'originaria promessa democratica.

L'infosfera è oggi attraversata da molteplici forme di reato

Revenge porn, abusi filmati, la sexortion richiesta dai caratteri estorsivi che si rivolta soprattutto ai minori, sotto la "Lente" del Garante sono finite diverse fattispecie che si consumano nell'infosfera, categoria in cui reale e virtuale sono categorie dell'essere ormai inseparabili. Con quali conseguenze?

Riprendo le parole di Umberto Eco: La micro-celebrità che assicura il web, con il mito di influencer seguiti da milioni di follower, sembra poter liberare da quello che, soprattutto ai ragazzi, appare uno "spaventoso e insopportabile anonimato". Bisogna comprendere questa dinamica psicologica per capire il rapporto osmotico, e spesso inconsapevole, che i ragazzi intessono con le nuove tecnologie. Il paradosso di voler riprodurre on line la propria vita, anche al prezzo di quella degli altri, come nel caso del bimbo travolto, lo scorso giugno, dall'auto in corsa di alcuni youtuber, nella loro ricerca spasmodica di un like in più, si spiega in questo orizzonte perverso che confonde: valori, categorie, dimensioni dell'essere. Quest'alienazione dal reale è il frutto della virtualizzazione della vita, componente difficile da governare, in cui si rischia di confondere la persona con l'avatar, finendo col ridurre anche la percezione del "male", di cui la rete offre spesso una "narrazione pornografica".

Ogni percezione della sofferenza sfuma, quasi la vita si consumasse in un perenne videogame. Una malattia difficile da curare, non crede?

Direi di più sembra attenuarsi, fin quasi a scomparire, quel "sentimento supremo", quella "telepatia delle emozioni" che Milan Kundera identificava nella compassione intesa, etimologicamente, come capacità di "sentire" l'altrui sofferenza. Il legame tra minori, violenza e rete racconta molto del nostro presente e delle distorsioni cui può condurre la congiunzione tra povertà etico/affettivo/educativa e sottovalutazione degli effetti della rete. Il malinteso anonimato del web, così come la defisicizza-

zione dei rapporti, (fenomeno che avviene quando l'altro è ridotto a immagine, profilo, avatar) sono fattori che alimentano, soprattutto nei giovani, quell'aggressività che spesso nella vita offline incontra il limite dell'inibizione e la deterrenza del controllo sociale, penso al cyberbullismo. Non dimentichiamo che lo stesso termine "violenza" tiene insieme, i termini greci: "βίος" che significa vita e "βία" che vuol dire violazione del limite, delle regole, come a sottolineare questo tempo dell'eccedenza, insieme al meccanismo d'interdizione che sono sottesi all'esercizio della violenza.

Chiedo in conclusione: cosa si può fare per interrompere la dilagante escalation di reati?

Dobbiamo utilizzare tutta la conoscenza, la consapevolezza e la competenza di cui siamo capaci per illuminare il lato oscuro della rete, rendendola, come dicevo prima, quello strumento di libertà, pluralismo e democrazia che dovrebbe costituirne il DNA. In questo percorso è necessario mettere in campo una pedagogia digitale che è - per l'istituzione che ho l'onore di presiedere - una priorità, un tassello necessario della formazione dei futuri cittadini, che devono comprendere che proteggere i dati, che attengono alla propria sfera personale, vuol dire difendere la libertà come valore indefettibile, scongiurando il pericolo incombente, di divenire, come ha scritto molto bene Michele Serra, schiavi della "dittatura della presenza".

CYBER
Think Tank
ASSINTEL

CYBER
Think Tank
ASSINTEL

Collabora, Inventa, Proteggi

Entra nel nostro Cyber Think Tank !

Cyber Think Tank Assintel

Prossimo Incontro

10 LUGLIO

14:00 - 15:30

Per info scrivi a:
segreteria@assintel.it

Garantire la sicurezza degli oggetti grazie all'Identity of Things

A cura di Danilo Cattaneo

Nel mondo digitale, oramai pervasivo e in costante e rapida evoluzione, la sicurezza informatica è una priorità fondamentale. Questo concetto, seppur ampiamente riconosciuto non più solo dagli esperti di settore ma chiaro ai policy makers e ai leader d'azienda, continua a non essere oggetto di attenzione sufficiente da molte organizzazioni, in ogni settore. Lo dimostra il recente Assintel Cyber Report che dipinge un quadro allarmante: nel 2023 +184% di cyber attacchi nel mondo. Il 61% viene dal dark web, il 70% sono malware; in Italia il numero di attacchi nel secondo semestre (H2) è significativamente aumentato rispetto al primo semestre e secondo trimestre, indicando un aumento della minaccia del ransomware nel corso dell'anno.

Questo dato in crescita non colpisce solo il settore IT, ma coinvolge anche sistemi e reti OT (Operation Technology), utilizzati per il controllo di dispositivi industriali e infrastrutturali, in diversi settori, come quello manifatturiero, energetico, trasporti e sanitario.

Si osserva, inoltre, un trend sempre crescente nel condividere in rete gli oggetti, il cosiddetto Internet of Things (IoT), che amplia la capacità dei dispositivi di raccogliere, elaborare e condividere dati, consentendo un miglioramento nel monitoraggio, controllo e automazione di processi. La crescente interconnessione di reti e infrastrutture critiche con sistemi centralizzati o altri ecosistemi tecnologici è alimentata dalla tendenza dell'Internet of Things (IoT) che sta trasformando numerosi settori in "smart", come le Smart Cities, la Smart Mobility, le Smart Grid, la Smart Health e la Smart Industry.

Tuttavia, se da un lato queste innovazioni consentono efficienza e miglioramenti nei servizi, dall'altro aumentano il perimetro di attacchi cyber esponendo le aziende a una potenziale minaccia su infrastrutture vitali, con possibili impatti gravi sulla sicurezza e la vita di milioni di persone.

Di fronte a questo scenario, una domanda sorge spontanea: quali misure si possono adottare per ridurre il rischio degli effetti malevoli di un cyber attacco a infrastrutture critiche?

Non esiste una risposta unica, in quanto il panorama delle soluzioni di Cybersecurity OT è vario e complesso, ma vi sono delle Best Practices che possono essere facilmente esportate da mondi adiacenti.

Ad esempio, nel contesto del Digital Trust, la gestione dell'Identità Digitale delle persone fisiche e delle entità legali regolata dal regolamento eIDAS, rappresenta un elemento fondamentale. Garantendo un'identificazione certa, infatti, si abilitano numerosi altri servizi e processi che aumentano la sicurezza sia delle imprese e degli individui coinvolti.

Spesso però manca una gestione certa "dell'Identità delle Cose" nel mondo OT: l'Identity of Things, emersa parallelamente all'Internet of Things, infatti non riceve spesso l'attenzione necessaria, forse anche per l'assenza di un quadro normativo specifico nel settore dell'IoT Security.

Alcuni settori sono tuttavia precursori, intraprendendo iniziative come ad esempio il comparto elettrico che ha sviluppato e adottato gli standard IEC 62351: IEC è la Commissione elettrotecnica internazionale, una organizzazione internazionale deputata a definire standard in materia di elettricità, elettronica e tecnologie correlate. Gli standard IEC 62351 sono stati sviluppati per gesti-

re la sicurezza nelle fasi di autenticazione del processo di trasferimento di dati tra dispositivi di trasmissione elettrica, garanzia di accessi esclusivamente dopo autenticazione, prevenzione di intercettazioni della comunicazione non autorizzate, garanzia di confidenzialità, prevenzione di attacchi e rilevamento di intrusioni.

Ancora, nel campo della Smart Mobility sono state emanate dal Governo del Regno Unito le normative "The Electric Vehicles (Smart Charge Points) Regulations 2021", con l'obiettivo di gestire l'aumento della domanda di elettricità nella transizione verso i veicoli elettrici, al contempo garantendo la sicurezza dei punti di ricarica presenti sulle strade del Regno.

Questi due esempi evidenziano una prima tendenza di intervento, tuttavia c'è ancora molto da fare per garantire la sicurezza di tutte le infrastrutture critiche, in un contesto che diventa sempre più interconnesso e digitale.

Leggendo in controluce le normative e gli standard esistenti, si individua un pattern comune: una soluzione di IoT security efficace deve includere una serie di misure proattive per proteggere le identità delle macchine, come:

- l'autenticazione forte dei dispositivi IoT;
- la crittografia end-to-end per proteggere i dati in transito;
- la segmentazione di rete per limitare l'accesso non autorizzato e la costante sorveglianza e rilevamento delle minacce per identificare e rispondere prontamente a eventuali intrusioni.

Il tutto meglio se gestito da fornitori affidabili, ovvero "terze parti" certificate e referenziate o partner di fiducia, così che possano garantire la sicurezza end-to-end dei dispositivi IoT. A volte, tali indicazioni provengono dagli stessi standard e protocolli di comunicazione, nel settore dello Smart Charge, ad esempio, è generalmente usato il protocollo di comunicazione sviluppato dalla Open Charge Alliance, chiamato OCPP.

Nel mondo digitale, oramai pervasivo e in costante e rapida evoluzione, la sicurezza informatica è una priorità fondamentale.

Il protocollo OCPP prevede un'estensione di sicurezza che richiede l'uso certificati PKI, comunicazioni cifrate e consiglia di affidarsi a terze parti definite Trusted Third Parties.

PKI, acronimo di Public Key Infrastructure, è la tecnologia alla base dei certificati digitali, ad esempio ai certificati di firma digitale o di sigillo oggi rilasciati a persone fisiche o persone giuridiche. Un certificato digitale è un documento che autentica l'identità e garantisce sicurezza nell'autenticazione, l'identificazione e, eventualmente, sottoscrizione di un payload. Nel contesto dell'IoT, l'implementazione di una PKI garantisce in modo affidabile l'identità di qualsiasi dispositivo connesso a una rete. Ciò assicura l'autenticità e l'integrità dei dati scambiati nelle comunicazioni machine-to-machine, proteggendo contemporaneamente il canale di comunicazione.

Questo è solo un esempio delle molteplici applicazioni delle tecnologie di sicurezza nell'ambito dell'IoT, tecnologie che, sebbene non nuove, spesso non vengono pienamente adottate. Troppo spesso, le imprese e gli enti sfruttano solo parzialmente le potenzialità innovative dell'IoT, rimandando l'implementazione di soluzioni di sicurezza robuste fino alla necessità normativa o, peggio ancora, fino a che non si verifichi un attacco informatico.

Non è possibile sfruttare appieno i vantaggi delle innovazioni come l'Internet of Things senza investire nel miglioramento dei livelli di sicurezza.

Garantire l'Identity of Things è un elemento fondamentale di questa linea di azione.

La cyber security al centro - i paradigmi dell'industria di oggi e domani

A cura di Marco Comastri

L'industria moderna è in costante evoluzione, attraversando fasi di trasformazione tecnologica che pongono nuove sfide, ma al contempo offrono opportunità uniche.

Con l'avvento della digitalizzazione e la crescente interconnessione delle attività aziendali, la cyber security emerge come un pilastro fondamentale, garantendo non solo la protezione dei dati, ma anche la competitività e la resilienza delle aziende, indipendentemente dalla loro dimensione o settore.

D'altronde, l'era della digitalizzazione ha segnato un'epoca di produttività aumentata attraverso l'integrazione di Big Data, tecnologie IoT e sistemi intelligenti. Tuttavia, l'adozione di nuove tecnologie rappresenta un passo avanti che richiede un approccio più umano, sostenibile e resiliente. Questo cambiamento non è solo tecnologico, ma anche culturale, e la sicurezza informatica deve essere integrata in ogni fase di questo nuovo paradigma aziendale.

Oggi, e sempre di più nel futuro, la collaborazione tra uomo e macchina si intensifica, creando una superficie di attacco più ampia e complessa. La crescente interconnessione tra dispositivi IoT, sistemi di realtà aumentata e altre tecnologie richiede misure di sicurezza più robuste per proteggere i dati sensibili e prevenire attacchi informatici. La sicurezza informatica non è più un'opzione, ma una necessità integrata in ogni fase del processo aziendale.

Sfide e opportunità

La gestione della sicurezza informatica nei nuovi ambienti aziendali deve affrontare diverse sfide. Uno dei principali problemi della trasformazione digitale dell'ultimo decennio è stato lo sviluppo di sistemi con vulnerabilità intrinseche, spesso dovute all'utilizzo di software obsoleti. Molte aziende, ad esempio, ancora utilizzano sistemi operativi datati che richiedono protezioni specifiche per minimizzare i rischi. In questo contesto, l'adozione di normative come la direttiva NIS2 e il Cyber Resilience Act a livello europeo mira a rafforzare la sicurezza dei prodotti digitali connessi e a garantire che tutte le aziende, dalle piccole e medie imprese (PMI) ai grandi gruppi, implementino misure di sicurezza efficaci. Questi regolamenti stimolano una maggiore maturità cyber all'interno delle organizzazioni, spingendole verso pratiche più sicure e resilienti.

La formazione del personale è un altro aspetto cruciale per il successo delle imprese in questa nuova era digitale. Gli operatori devono essere consapevoli dei rischi informatici e sapere come rilevare e rispondere agli attacchi. La sensibilizzazione e l'educazione sulla cyber security devono diventare parte integrante della cultura aziendale, affinché i dipendenti possano reagire prontamente a qualsiasi anomalia nei sistemi. In Italia, la cyber security non è solo una questione di protezione dei dati, ma anche di competitività economica. Come evidenziato da esperti del settore, maggiore sicurezza significa maggiore competitività sul mercato. Questo è particolarmente rilevante per le PMI, che rappresentano la spina dorsale dell'economia italiana. Un'azienda che investe in cyber security non solo protegge i propri asset, ma rafforza la propria posizione competitiva, contribuendo così allo sviluppo economico del paese. È anche vero che le competenze richieste in questo nuovo panorama sono

sempre più specializzate. La domanda di professionisti STEM (Science, Technology, Engineering, Mathematics) è in continua crescita, ma non bisogna trascurare l'importanza dei profili umanistici. In un'epoca di trasformazione digitale, la formazione continua è essenziale. Le aziende devono investire nella formazione del proprio personale, offrendo percorsi di apprendimento che combinano competenze tecniche e umanistiche per affrontare le sfide della cyber security. Non sarebbe errato dire che proteggere l'economia significa anche contribuire al benessere della società. La cyber security è un settore in continua evoluzione, che richiede un approccio dinamico e collaborativo.

L'intelligenza artificiale, per esempio, offre strumenti potenti per migliorare la sicurezza, ma rappresenta anche una minaccia se utilizzata dagli attaccanti. È quindi fondamentale sviluppare competenze avanzate e promuovere una cultura della sicurezza in tutta l'organizzazione. La cyber security nell'era digitale, quindi, non è solo una questione di tecnologie e protocolli, ma di persone e competenze.

La collaborazione tra i vari dipartimenti aziendali, la formazione continua del personale e l'adozione di nuove tecnologie sono elementi chiave per costruire un ambiente sicuro e resiliente. Mentre ci muoviamo verso un futuro sempre più connesso e digitale, la cyber security deve essere al centro delle strategie aziendali, garantendo che i sistemi siano non solo efficienti e produttivi, ma anche sicuri e resilienti. La protezione dei dati e la sicurezza dei sistemi operativi sono fondamentali per costruire la fiducia necessaria tra uomo e macchina, pilastro della nuova era digitale.

CYBER
Think Tank
ASSINTEL

La cyber security è un settore in continua evoluzione, che richiede un approccio dinamico e collaborativo.

AI Act: il Regolamento europeo in materia di Intelligenza Artificiale

A cura di Ranieri Razzante

L'intelligenza artificiale è una realtà che si sta sviluppando sempre più velocemente e che già sta impattando sul nostro modo di vivere. Proprio per questo l'Unione europea ha avvertito la necessità di regolarne l'utilizzo.

Visti i grandi cambiamenti tecnologici in corso e le possibili nuove sfide, l'UE si impegna, mediante un intervento legislativo che assicuri il buon funzionamento del mercato interno, affinché sia i benefici che i rischi legati all'uso dei sistemi di intelligenza artificiale siano affrontati e distribuiti in modo adeguato a livello europeo. L'obiettivo principale è quello di sviluppare un'intelligenza artificiale sicura, etica ed affidabile.

Dal punto di vista normativo, il Regolamento europeo sull'intelligenza artificiale (AI Act) è il primo quadro giuridico assoluto in questa materia, ed è stato considerato uno step fondamentale per il futuro digitale dell'Europa. L'AI Act nasce da una proposta di Regolamento presentata dalla Commissione europea nell'aprile del 2021, con lo scopo di creare un quadro normativo apposito per l'intelligenza artificiale nell'Unione Europea.

Dopo anni di negoziazioni, il 13 marzo 2024 il testo è stato approvato dal Parlamento europeo. Tuttavia, le norme del Regolamento non saranno immediatamente applicabili. È, infatti, previsto un cuscinetto di 24 mesi (nella versione di Commissione e Parlamento) o di 36 mesi (nella posizione del Consiglio).

Con la presente proposta si tiene fede all'impegno politico della presidente Von Der Leyen che, nei suoi orientamenti per la Commissione 2019 – 2024, ha annunciato che la stessa avrebbe presentato una normativa per un approccio europeo coordinato con le implicazioni umane ed etiche dell'intelligenza artificiale.

A tal proposito, la Commissione ha pubblicato il 19 febbraio 2020 il Libro Bianco sull'intelligenza artificiale, promuovendo un approccio europeo all'eccellenza e alla fiducia.

L'AI dovrebbe rappresentare unicamente uno strumento utile per le persone e per la società, con il fine di migliorare il benessere degli esseri umani.

La proposta in questione mira a sviluppare un quadro giuridico per un'AI affidabile, basandosi, in primis, sui diritti fondamentali e prefiggendosi di dare ai cittadini la fiducia per adottare soluzioni basate sull'AI stessa.

Il Regolamento fissa delle regole armonizzate per lo sviluppo del rischio, l'immissione sul mercato e l'utilizzo di sistemi di AI nell'Unione europea seguendo un approccio basato sul rischio.

L'AI Act si inserisce nell'ambito della c.d. strategia "a Europe fit for the digital age" (un'Europa adatta all'era digitale), delineata dalla Commissione Europea.

L'articolo 3 del testo definisce l'intelligenza artificiale

come “Un sistema basato su macchine progettato per operare con vari livelli di autonomia e che può mostrare adattabilità dopo il dispiegamento e che, per obiettivi espliciti o impliciti, deduce dagli input ricevuti come generare output quali previsioni, raccomandazioni di contenuti o decisioni che possono influenzare ambienti fisici o virtuali”. Una definizione che può essere usata oggi tra le tante che ne sono state via via fornite.

La nuova legge si applicherà a tutti i soggetti, pubblici e privati, all’interno e all’esterno dell’Unione. L’AI Act segue un approccio per l’appunto basato sul rischio, dividendo i sistemi di intelligenza artificiale sulla base di quattro categorie: minimo, limitato, alto e inaccettabile. Maggiore è il rischio, maggiori sono le responsabilità ed i limiti per chi usa questi sistemi, fino ad arrivare ai modelli troppo pericolosi per essere utilizzati.

Tra gli impieghi vietati si trovano le tecnologie subliminali per manipolare i comportamenti delle persone, la categorizzazione biometrica, la raccolta di foto di volti da internet, i sistemi di punteggio sociale o social scoring e la polizia predittiva, cioè l’uso di dati sensibili per calcolare le probabilità che una persona commetta un reato. Su quest’ultimo utilizzo, per il vero, occorrerà fare chiarezza.

Le aziende dovranno, quindi, iniziare a valutare gli impatti dell’AI Act sulla propria attività, implementando strategie di governance e adottando politiche per conformarsi alle previsioni del Regolamento, con lo scopo di prevenire i rischi e sfruttare le opportunità che l’AI Act apporterà nel mercato.

I sistemi di intelligenza artificiale dovranno essere: trasparenti, sicuri, tracciabili, non discriminatori e rispettosi della privacy. Requisiti chiari e irrinunciabili.

L’intelligenza artificiale è una realtà che si sta sviluppando sempre più velocemente e che già sta impattando sul nostro modo di vivere.

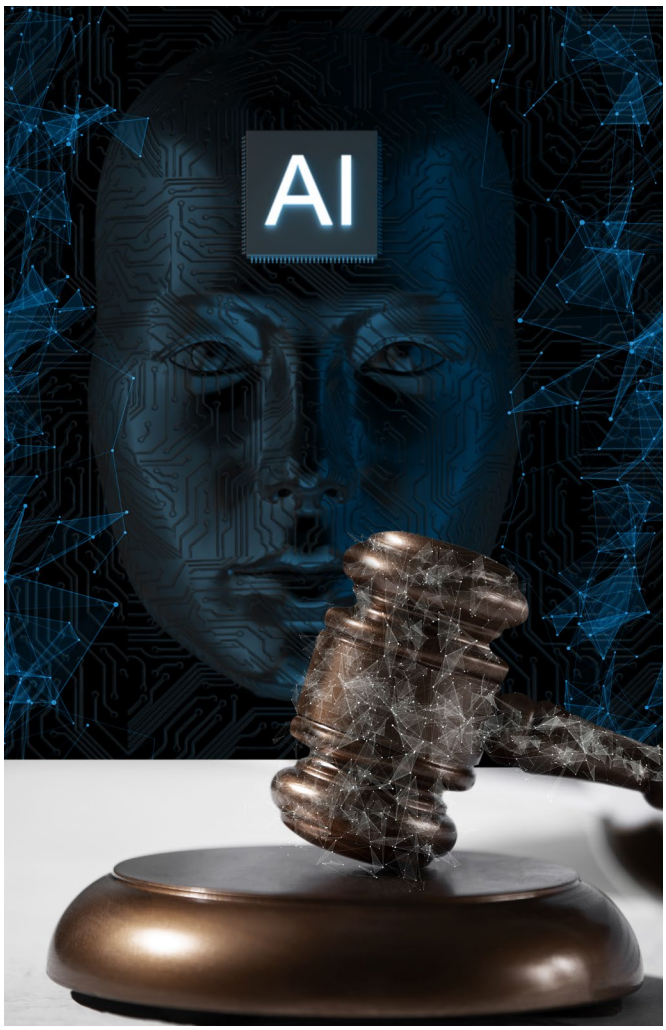
Il Regolamento prevede, in sintesi;

- regole per l’immissione sul mercato, la messa in servizio e l’uso dei sistemi di intelligenza artificiale nell’Unione europea;
- divieti di alcune pratiche di AI;
- misure per sostenere l’innovazione, con particolare attenzione alle *start-up*;
- regole di trasparenza per i sistemi di AI;
- requisiti specifici per i sistemi di AI ad alto rischio e obblighi per i loro operatori;
- regole su monitoraggio del mercato, vigilanza del mercato, governance ed esecuzione.

L’AI Act si basa su un approccio che fa riferimento a due principi fondamentali: la fiducia e l’eccellenza. Entrambi gli elementi sono importanti per far sì che l’intelligenza artificiale entri in contatto con tutti i cittadini in modo sicuro.

L’utilizzo dei sistemi di AI scandisce il futuro che vivremo. I sistemi di intelligenza artificiale devono essere utilizzati correttamente da tutti i cittadini, per far sì che si possa davvero parlare di fiducia nell’AI.

Lo scopo principale è quello di promuovere “un’Europa resiliente per il decennio digitale”, dove tutte le imprese riescano a usufruire dei vantaggi offerti dell’intelligenza artificiale, sentendosi, al tempo stesso, protetti e sicuri. L’entrata dell’AI Act segnerà senza dubbio un traguardo significativo per il progresso dell’intelligenza artificiale nell’ambito dell’Unione europea. Si tratta di una sfida difficile ma, allo stesso tempo, essenziale.



Costruire Ponti Digitali: l'interoperabilità nella lotta contro le minacce informatiche

A cura di Sandra Marsico

Ormai non si può iniziare una dissertazione su argomenti inerenti la cyber security senza un doveroso preambolo: l'ecosistema digitale odierno è caratterizzato da minacce informatiche in continua evoluzione e sempre più sofisticate, perimetri di sicurezza che si estendono oltre i confini tradizionali, organizzazioni che implementano una vasta gamma di soluzioni di sicurezza e un bisogno sempre più impellente di affrontare la sicurezza in modo olistico o, come si suol dire, come un "tutto".

È in questo panorama che l'interoperabilità tra gli strumenti di cybersecurity emerge come una necessità imperativa per il raggiungimento di diversi obiettivi, tra i quali:

- **Affrontare in modo efficace e tempestivo gli attacchi informatici, massimizzando l'efficienza delle risorse e riducendo i tempi di risposta.**

  Ricordiamoci che il Dwell Time (tempo di permanenza) medio globale relativamente alla persistenza degli attaccanti all'interno delle infrastrutture delle vittime, è sì in continuo calo, anno dopo anno, ma che è ancora a dei livelli pericolosamente elevati. Secondo l'ultimo rapporto M-Trends 2023 il numero medio di giorni in cui un attaccante è rimasto sottotraccia nell'ambiente target prima di essere rilevato, è stato di 16 giorni nel 2022.

- **Utilizzare in modo più efficiente le risorse, sia in termini di hardware/software che di risorse umane.**

  Evitare quindi sovrapposizioni in termini di funzionalità erogate o espletate, ridurre gli interventi manuali, permettendo alle organizzazioni di destinare i propri dipendenti a compiti che richiedono maggiore attenzione strategica. Potremmo dire compiti più di concetto e meno esecutivi. E questo ci porta al terzo obiettivo.

- **Potenziare l'efficienza operativa e l'automazione attraverso l'ottimizzazione dei processi di sicurezza.**

  Per fare degli esempi molto semplici, parliamo in questo caso di attività quali scansioni delle vulnerabilità, distribuzione di patch e, come indicato in precedenza, della risposta agli incidenti. Lo scopo è quello di rendere le operazioni più rapide ed efficienti.

L'interoperabilità si potrebbe definire come la capacità di interazione tra sistemi eterogenei, e si rivela essenziale per lo scambio efficace di dati e l'armonizzazione dei vari sistemi di protezione in campo che, nella maggior parte dei casi, vengono offerti da differenti produttori.

Questo concetto sostiene non solo una comunicazione continua e senza ostacoli tra piattaforme tecnologicamente diverse, ma offre inoltre la possibilità, per le entità che intendono perseguirla, di sviluppare una strategia di sicurezza informatica su misura, che si amalgama senza frizioni con la propria infrastruttura di sicurezza la quale, se pure basata sulle migliori best practice del settore, rimane naturalmente unica nel suo genere ed esclusiva dell'organizzazione.

Il raggiungimento di un' interoperabilità completa è al momento una sfida che, nonostante gli immensi progressi che si stanno raggiungendo in tal senso, appare ancora molto lontana dall'essere vinta. Le differenze tra le architetture dei sistemi, la varietà dei linguaggi di pro-

grammazione e l'esigenza di proteggere le informazioni sensibili, complicano l'integrazione.

Non da ultima, vi è la questione della volontà dei fornitori di collaborare nello standardizzare le loro soluzioni per il bene comune, superando la tendenza a creare ecosistemi chiusi. Se per le organizzazioni i benefici sono facilmente individuabili (in questo articolo ne abbiamo già citati tre, a mero titolo esemplificativo, ma ve ne sono molti di più), anche per i fornitori di soluzioni di sicurezza le opportunità che derivano da un maggior focus sull'interoperabilità non sono da sottovalutare. Una su tutte, la possibilità di distinguersi in un mercato competitivo, offrendo soluzioni che non solo siano potenti da sole ma possano anche amplificare l'efficacia delle tecnologie esistenti.

Mentre esploriamo le complessità e le sfide dell'interoperabilità nell'ambito della cybersecurity, emergono ulteriori considerazioni che ampliano la nostra comprensione su come affrontare efficacemente le minacce informatiche.

La distanza tra l'ambizione di un' interoperabilità completa e la realtà attuale ci spinge a riflettere non solo sulle barriere tecniche e sulla volontà dei fornitori, ma anche sul divario percettivo tra i produttori di software di sicurezza e le effettive necessità dei loro utenti finali. Questo divario risalta particolarmente quando consideriamo l'ampia gamma di utenti che interagiscono con le soluzioni di cybersecurity.

Tradizionalmente, si potrebbe pensare che il personale IT sia l'unico custode della sicurezza digitale di un'organizzazione. Tuttavia, la realtà è molto più sfaccettata. Organizzazioni vitali, come quelle che gestiscono l'infrastruttura critica nazionale o i sistemi industriali, si affidano spesso a specialisti non IT per implementare e gestire le loro strategie di cybersecurity. Questa pratica mette in luce l'importanza di sviluppare soluzioni interoperabili che siano non solo tecnicamente compatibili tra diversi sistemi, ma anche accessibili e utilizzabili da un'ampia varietà di professionisti.

La vera misura del successo di un prodotto di cybersecurity non si trova solamente nella sua capacità di soddisfare le esigenze tecniche del personale IT, ma nel suo impatto sulla leadership aziendale e sulle autorità che valutano la postura di sicurezza di un'entità.

Chief Information Security Officers (CISO) e altri responsabili della sicurezza devono allora superare una visione ristretta che si concentra esclusivamente sulle nuove funzionalità del software. È essenziale riconoscere che il valore di una soluzione di cybersecurity si estende ben oltre la sua efficienza operativa, abbracciando aspetti critici come la conformità normativa, la gestione del rischio e la mitigazione delle vulnerabilità.

Collegando questi concetti, diventa evidente che l'interoperabilità e l'adattabilità delle soluzioni di cybersecurity non devono solo facilitare la comunicazione tecnica tra diversi sistemi. Devono anche rispecchiare una comprensione profonda delle variegate necessità degli utenti finali e delle strutture organizzative. Solo attraverso un approccio inclusivo e olistico, che riconosce l'importanza di soddisfare le esigenze di un'ampia gamma di stakeholder, si può veramente avanzare verso un ecosistema di cybersecurity più resiliente ed efficace.

Solo attraverso sforzi congiunti e un impegno verso l'integrazione e la cooperazione possiamo sperare di costruire un ambiente digitale più sicuro per tutti.

Arrivati a questo punto di comprensione del perché andrebbe perseguita l'interoperabilità, chi ne beneficerebbe e a che livello, nasce spontanea una domanda: quali sono gli strumenti che, ad oggi, hanno gettato, e stanno gettando, le basi per la realizzazione di un'architettura interoperabile?

Tecnologie SIEM: le piattaforme di Security Information and Event Management (SIEM) aggregano dati di log provenienti da una varietà di fonti, inclusi computer e server basati su sistemi operativi Windows e Unix like,

dispositivi di networking, applicazioni (custom e di terze parti), e innumerevoli altre sorgenti fino ad arrivare ai controllori logici programmabili (PLC). Questi sistemi facilitano l'interoperabilità attraverso l'unificazione dei formati di log, applicando metodi di filtraggio, analisi e standardizzazione dei vari campi dati (con la normalizzazione del formato della data che rappresenta un vantaggio significativo già di per sé).

Tecnologie SOAR: i Security Orchestration, Automation, and Response (SOAR) sono soluzioni informatiche già progettate allo scopo di ottimizzare le operazioni di sicurezza. Integrano diversi strumenti, automatizzano i compiti ripetitivi e coordinano le risposte agli incidenti informatici. Il loro utilizzo migliora l'efficienza dei team di sicurezza, riduce i tempi di risposta alle minacce e aumenta l'efficacia complessiva della gestione degli incidenti di sicurezza. È doveroso dire che, anche se nati per gli ambiti di cybersecurity, i SOAR vengono oggi utilizzati in modo proficuo anche in altri settori.

Tecnologie EDR/XDR: Endpoint Detection and Response (EDR) ed Extended Detection and Response (EDR) sono tecnologie di sicurezza che forniscono visibilità e difesa contro le minacce informatiche. Gli EDR si concentrano sulla protezione dei singoli endpoint, come computer e dispositivi mobili, monitorando e rispondendo a comportamenti sospetti. Gli XDR estendono questo concetto, integrando dati e segnali di allarme da più fonti, come reti, cloud ed endpoint, per offrire una visione olistica delle minacce e facilitare una risposta coordinata. Entrambi migliorano significativamente la capacità di rilevare, indagare e neutralizzare le minacce in tempo reale, rafforzando la postura di sicurezza complessiva. Similmente (ma senza potersi sostituire ad esse) alle tecnologie SIEM, queste tecnologie contribuiscono all'interoperabilità consolidando dati da fonti diverse.

STIX e TAXII: Structured Threat Information eXpression (STIX) e Trusted Automated eXchange of Indicator Information (TAXII) sono standard progettati per facilitare lo scambio di informazioni su minacce informatiche in modo strutturato e automatizzato. STIX definisce come rappresentare le informazioni sulle minacce, mentre TAXII stabilisce il protocollo per lo scambio di tali informazioni. Insieme, migliorano la collaborazione tra le varie entità nella lotta (troppo spesso impari) contro le minacce informatiche, consentendo condivisione rapida e affidabile di intelligence sulla sicurezza.

YARA RULES: le Yara Rules sono un insieme di criteri utilizzati per identificare e classificare malware e altre minacce informatiche attraverso la scansione di file o flussi di dati. Queste regole permettono agli analisti di sicurezza di definire pattern specifici, come sequenze di byte o stringhe testuali, che corrispondono a caratteristiche note di software identificati come dannosi.

API: le Application Programming Interfaces (API) sono insiemi di regole e definizioni che consentono a software diversi di comunicare tra loro. Fungono da intermediari, permettendo alle applicazioni di scambiare dati e di richiedere servizi in modo efficiente e sicuro (se sviluppate in nome della security by design). L'uso delle API facilita l'integrazione e l'automazione tra diverse piattaforme e servizi, migliorando la flessibilità e l'espandibilità delle applicazioni, e contribuendo allo sviluppo di ecosistemi tecnologici più connessi e interfunzionali.

Le tecnologie citate, tendenzialmente espongono o si avvalgono di API per fornire le funzionalità di interoperabilità di nostro interesse.

Molti fornitori offrono accesso di terze parti a un set (seppur limitato) di risorse nei loro prodotti software tramite interfacce API.

Purtroppo, non esiste ad oggi una standardizzazione nelle strutture dei messaggi o nelle risposte, portando a differenze nel design e nei set di funzionalità tra i vari fornitori.

La notizia positiva è che iniziative come lo sviluppo di standard di settore più coerenti e la promozione di una cultura di collaborazione tra fornitori e organizzazioni utenti stanno gettando le fondamenta per un futuro in cui l'interoperabilità non sia solo possibile, ma diventi la norma.

L'adozione di tecnologie interoperabili rappresenta una pietra miliare cruciale nella lotta contro le minacce informatiche. Man mano che ci muoviamo verso questo obiettivo, è fondamentale che tutti gli attori coinvolti - dalle aziende tecnologiche ai decisori aziendali, fino agli stessi professionisti della sicurezza - riconoscano il valore e il potenziale di un approccio unitario alla cybersecurity.

Solo attraverso sforzi congiunti e un impegno verso l'integrazione e la cooperazione possiamo sperare di costruire un ambiente digitale più sicuro per tutti.

WEBINAR

AI & Cyber

CYBER Think Tank ASSINTEL

Settembre

12:00 - 13:00

Relatori:

Pierguido Iezzi

Angela Carpano

Maria Cucci

Per info scrivi a:

segreteria@assintel.it

Alfabetizzazione Cyber: l'approccio del Cyber Think Tank Assintel

A cura di Carlo Guastone

I Piani di cybersecurity in Italia

Il 15 gennaio 2018 il CINI (Cybersecurity national lab) ha pubblicato il documento: "Il futuro della cybersecurity in Italia - Progetti e Piani per difendere al meglio il paese dagli attacchi informatici" nel quale, con il contributo di 120 ricercatori di 40 enti di ricerca/università, si delineava lo stato dell'arte della cybersecurity in Italia con accenni al contesto internazionale, pubblicazione che costituisce tuttora un autorevole riferimento quando si parla di sicurezza cibernetica, pur considerando l'incessante evoluzione delle tecnologie e del quadro normativo registrata nel tempo. Basti pensare alla creazione di ACN (Autorità per la cibersicurezza nazionale) e alla pubblicazione di numerose normative di legge fra le quali il Perimetro di sicurezza nazionale, il NIS2 dedicato ai servizi essenziali, il Regolamento DORA dedicato alla resilienza nel settore finanziario, per finire al recentissimo AI Act dedicato all'Intelligenza artificiale, normative che presentano forti relazioni con la cybersecurity.

Nel 2022 ACN (Autorità per la cybersicurezza nazionale) ha definito la Strategia Nazionale di Cybersicurezza 2022-26, con un Piano, basato su 82 misure, fra le quali alcune misure destinate alla messa in campo di iniziative finalizzate a migliorare la conoscenza della cybersecurity e sensibilizzare i responsabili delle organizzazioni e di chi opera sul campo tramite strumentazione digitale.

La Misura #10 prevede di "Pubblicare linee guida sulla cybersecurity" specificamente previste per le Amministrazioni Pubbliche, e applicabili anche da parte delle aziende private; la Misura #11 è dedicata alla promozione di iniziative di sensibilizzazione per favorire l'applicazione del "Framework Nazionale per la Cybersecurity e la Data Protection" e dei "Controlli essenziali di cybersecurity", opportunamente aggiornati in linea con il quadro delle minacce cyber da parte della PA, delle imprese e delle PMI; la Misura #12 prevede di continuare ad accrescere le capacità nazionali di difesa, resilienza, contrasto al crimine e cyber intelligence, rafforzando ulteriormente la situational awareness mediante il monitoraggio continuo e l'analisi di minacce, vulnerabilità e attacchi, secondo gli specifici ambiti di competenza; la Misura #13 consiste nella realizzazione di un servizio di monitoraggio del rischio cyber nazionale a favore delle organizzazioni e del pubblico in generale, al fine di comunicare l'effettivo livello della minaccia, nonché di informare adeguatamente i processi decisionali.

Le iniziative del Cyber Think Tank Assintel

Di fronte ad uno scenario complesso che determina crescenti difficoltà delle aziende, in particolare le PMI, nel predisporre le necessarie misure organizzative, metodologiche e tecnologiche per rispondere a quanto previsto nel quadro normativo per minimizzare i rischi di sanzioni, e, soprattutto, per garantire la continuità del business, sempre più esposto a minacce cyber, sono state promosse una serie di iniziative in fase avanzata di realizzazione cui saranno dedicati specifici webinar di approfondimento.

La logica seguita dai componenti del Cyber Think Tank, che hanno una profonda e pluriennale esperienza consulenziale in area Cyber, è stata quella di identificare le aree di sensibilizzazione cyber destinate in particolare a non esperti della materia per favorire la comprensione

delle minacce e la predisposizione delle relative misure di mitigazione dei rischi, il tutto tramite una comunicazione il più possibile semplice ed efficace. Il risultato atteso dalla iniziativa è l'incremento di consapevolezza da parte dei responsabili di business della necessità di valutare i rischi cyber assegnando le conseguenti responsabilità all'interno dell'organizzazione con il ricorso a supporti consulenziali ove ritenuto opportuno o necessario.

Iniziative di sensibilizzazione identificate:

- **Assintel Cyber Hub** ha l'obiettivo di mappare ed elencare le aziende associate ad Assintel con competenze di ambito cyber al fine di offrire un punto di riferimento nell'identificazione di competenze, servizi e soluzioni di valore. Il Cyber Hub è una sorta di "catalogo" all'interno del quale ogni azienda partecipante avrà una propria scheda con le informazioni raccolte attraverso un questionario. Il Cyber Hub sarà arricchito da un Vademecum con le buone pratiche in ambito cybersecurity.
- **Cyber Threat Infosharing** è la piattaforma creata e messa a disposizione gratuitamente dal Cyber Think Tank a tutta la community ICT. Obiettivo della piattaforma è supportare le aziende nella gestione dei rischi cyber, offrendo una panoramica su campagna di phishing, malware, ransomware e vulnerabilità comuni (CVE). È uno strumento cruciale per le imprese che vogliono comprendere e mitigare le minacce informatiche in tempo reale, fornendo sezioni dedicate con i relativi IoC legati agli ultimi tentativi di phishing, attività di ransomware e malware.
- **Cyber per tutti** è l'iniziativa finalizzata alla creazione di una serie di elementi comunicativi fruibili con semplicità ed immediatezza per sensibilizzare il management delle PMI sottolineando che la Cybersecurity e la Protezione dei dati (in senso lato) sono elementi su cui è necessario investire, sia lato infrastrutturale, che formativo. Vari i format previsti: video, checklist, infografiche, fumetti e podcast.

Le iniziative descritte rispondono, fra l'altro, ad una esigenza sempre più condivisa da esperti di settore e dalle forze politiche di incrementare gli sforzi per ridurre il gap dell'Italia relative alle competenze relative al digitale e alla cybersecurity rispetto ai contesti internazionali di riferimento. Significativo, al riguardo, che nel recente convegno svolto il 18 marzo alla Camera dei deputati "AB…D. Il cammino dell'Italia verso l'alfabetizzazione digitale" sia stata proposta creazione di un'Agenzia per l'alfabetizzazione digitale che avrebbe come compito la definizione pratica dei piani di alfabetizzazione con la loro implementazione a livello nazionale e territoriale.

Neuroscienze, guerre cognitive e narrazioni digitali

A cura di Marco La Rosa

Oggi la guerra si fa sempre meno sul campo di battaglia e sempre più dentro la nostra mente, in un incessante bombardamento di migliaia di narrazioni manipolatrici dai social e dagli altri canali a cui il mondo digitale ci espone ogni secondo. E non si creda che questo nuovo modo di farla sia a bassa intensità e perciò non ci faccia poi così tanto male: anzi, forse ottiene più risultati e lascia più danni delle vecchie armi convenzionali.

Basta guardare ai risultati. I cinesi sono riusciti a indurre nei giovani americani un forte rifiuto a combattere tramite Tik Tok, Zelensky ha tirato su il morale del suo popolo grazie all'uso sapiente dei "meme" e, da ormai un decennio, una misteriosa agenzia per le ricerche in internet di San Pietroburgo porta avanti le "psyop", delle "operazioni psicologiche" volte a destabilizzare politicamente i paesi est europei con narrazioni false che fanno sapientemente leva su aspettative, pregiudizi e paure.

L'importanza delle narrazioni

La differenza tra le nuove forme di guerra e la propaganda bellica tradizionale sta tutta nell'inedita combinazione tra narrazioni, neuroscienze, psicologia, algoritmi, canali digitali e nuove tecnologie come l'intelligenza artificiale.

Perché ricorrere a qualcosa di così tradizionale come le narrazioni in scenari così ultratecnologici? Nel suo libro appena uscito: Neuroscienze della narrazione , lo storytelling nell'era delle neuroscienze e dell'intelligenza artificiale (Hoepli), il blogger e divulgatore scientifico Marco La Rosa ci ricorda che alcuni esperimenti neuroscientifici come quello degli psicologi Schachter e Singer nel 1962 dimostrano che gli esseri umani interpretano le loro emozioni (rabbia, paura, gioia, entusiasmo) non solo sulla base delle reazioni fisiologiche, ma soprattutto in riferimento al contesto psicosociale in cui si trovano.

Basta quindi esporre le persone alle forme di narrazione-interpretazione del reale più opportune per fare loro interpretare quello che stanno provando come rabbia o odio e dirigere poi queste emozioni verso l'obiettivo ed il nemico desiderato. E i nuovi canali digitali sono, grazie alla loro natura onnipervasiva, l'ideale per consegnare qualsiasi tipo di messaggio a dei target prestabiliti.

La Rosa continua la sua analisi mostrando alcune applicazioni concrete delle scoperte delle neuroscienze e della psicologia cognitiva per creare storie particolarmente efficaci nell'influenzare l'opinione pubblica, manipolare le percezioni e, in definitiva, ottenere vantaggi strategici controllando ciò che potremmo chiamare lo spazio narrativo di una nazione.

Disinformazione mirata e ingegneria sociale

All'atto pratico, come vengono attuate le guerre cognitive? La disinformazione è una delle armi più utilizzate. Gruppi di attori statali o non statali possono diffondere notizie false attraverso i social media, siti web compromessi o altri canali online per influenzare l'opinione pubblica o destabilizzare nazioni avversarie. L'intelligenza artificiale, in particolare, può essere utilizzata per creare fake colossali per nulla distinti dalla realtà, come nel caso del falso arresto di Donald Trump.

Più subdoli sono gli attacchi di ingegneria sociale, che implicano la manipolazione psicologica degli utenti per ottenere informazioni sensibili o per condurli a compiere azioni dannose. Questa tattica è spesso utilizzata per infiltrarsi in reti sicure o per diffondere malware. Sarà così possibile atterrare interi servizi essenziali del paese nemico, dalle ferrovie alle poste, agli ospedali. Attacchi

del genere si sono verificati anche in Italia.

L'ingegneria sociale viene utilizzata persino nel cyber spionaggio: l'accesso non autorizzato a sistemi governativi, aziendali o militari può fornire informazioni vitali che possono essere sfruttate a fini politici, economici o militari.

Orientamento e persuasione dell'opinione pubblica

Il vero, grande, obiettivo di una guerra cognitiva resta, comunque, spostare l'opinione pubblica del paese target verso determinate posizioni politiche, o a sostegno di politici amici della nazione che porta avanti l'attacco.

Un governo che è stato spesso accusato di interferire in modo piuttosto pesante nelle elezioni di paesi dell'area dell'Unione europea e degli stessi Stati Uniti è quello russo. Questo tipo di attacco cognitivo non fa leva sulla vecchia carta stampa, o l'obsoleta strategia della tensione, ma sui social, i media digitali e, nel caso della campagna di Hillary Clinton (almeno, secondo quanto riportato dal giornalista Kevin Carboni su Wired il 14 settembre 2022), nell'hackeraggio delle e-mail dei suoi sostenitori.

Liquefazione della società del paese nemico

Il tipo di psyop più pericolosa resta tuttavia quella che mira a distruggere la fiducia della popolazione nello stato e nei suoi rappresentanti.

Un esempio potrebbe essere sabotare sistematicamente e occultamente con attacchi informatici i servizi essenziali come gli ospedali e i trasporti, accompagnando il tutto con violente campagne di stampa sull'inefficienza del sistema. Oppure esporre la popolazione a continui messaggi sulla corruzione e la criminalità dilagante, evidenziando l'incapacità delle autorità competenti di assicurare l'ordine per la loro inefficienza e impreparazione.

Una società sfiduciata, depressa e divisa tenderà infatti a reagire poco o nulla, diventando un nemico poco temibile e tendenzialmente neutralizzato.

Il problema della difesa cognitiva

Nel suo libro, La Rosa solleva infine il problema della libertà cognitiva, intesa come diritto a non essere manipolati, e della necessità di politica di difesa più attive e mirate da questo tipo di operazioni.

Su questa linea si stanno muovendo non solo istituzioni come l'Unione Europea, ma anche gli stessi governi. Purtroppo, costruire politiche di difesa efficaci è oggi molto difficile, sia per la difficoltà di tracciare e colpire questo tipo di attacchi, sia per la complessità delle tecnologie in gioco.

Un punto però è sicuro: in un mondo sempre più interconnesso, la sicurezza informatica diventa una frontiera cruciale nella difesa contro le guerre cognitive. Le organizzazioni governative, le aziende e gli individui devono adottare pratiche avanzate di cybersecurity per proteggere le proprie reti e dati sensibili.

Ciò include l'implementazione di sistemi avanzati di rilevamento delle minacce, la formazione continua del personale per riconoscere le tattiche di ingegneria sociale e la collaborazione internazionale per affrontare minacce transnazionali, e, perché no, maggiori competenze di comunicazione e contropropaganda negli esperti di sicurezza.

"Oggi la guerra si fa sempre meno sul campo di battaglia e sempre più dentro la nostra mente, in un incessante bombardamento di migliaia di narrazioni manipolatrici dai social e dagli altri canali a cui il mondo digitale ci espone ogni secondo."

Direttiva NIS2 (e direttiva CER) opportunità per le imprese, solo se gestita bene

A cura di Alessandro Manfredini

Circa un mese fa è stata pubblicata in Gazzetta Ufficiale la legge di delega al governo per il recepimento della Direttiva NIS 2, relativa alle misure per un livello comune elevato di cybersicurezza, e la Direttiva CER relativa alla resilienza dei soggetti critici, disposizioni normative che si aggiungono a quanto già indicato nel Regolamento Dora, relativo alla resilienza operativa digitale per il settore finanziario.

Il tempo a disposizione non è molto, visto che i termini scadono a ottobre. Le sfide, invece, sono tante. Basti pensare al necessario raccordo con le altre normative come il Perimetro di Sicurezza Nazionale Cibernetica e la (ormai ben nota) normativa sulla privacy.

Dalla prima lettura ci si aspettano effetti importanti soprattutto sulle piccole e medie imprese che potrebbero essere inserite tra i soggetti essenziali o soggetti importanti (novità appunto della Direttiva NIS2), senza contare che tra le altre novità c'è il coinvolgimento della supply chain, pertanto è verosimile che le imprese non designate potrebbero comunque essere coinvolte in quanto provider (come si dice "quello che non entra dalla porta entra dalla finestra").

Per questo serve un confronto tecnico strutturato con gli operatori e con chi potrebbe rappresentarli (dunque le associazioni) perché dobbiamo tenere conto del panorama e del tessuto economico del nostro Paese che è sicuramente diverso dagli altri Stati appartenenti alla Comunità Europea. Così se è vero che la EU ha inteso innalzare i livelli di sicurezza cyber all'indomani della crisi pandemica, adeguando ad esempio i settori ritenuti essenziali e importanti, non possiamo non tenere conto delle peculiarità del livello di industrializzazione e digitalizzazione, molto peculiare, del nostro Paese.

È urgente dunque definire una corretta migrazione da NIS a NIS2, anche se in realtà questo preoccupa meno, perché i soggetti in perimetro già oggi sono sicuramente più maturi; quella che veramente non deve essere sottovalutata è la corsa che dovranno fare le imprese passando direttamente alla NIS2 (i nativi 2.0!)

Infatti le prime stime ci indicano che i soggetti interessati passeranno da un migliaio a decine di migliaia e coinvolgeranno settori in cui i livelli di consapevolezza in materia cyber sono molto diversi.

Penso che sia poco realistico immaginare che nei tempi indicati tutte le Aziende saranno in grado di implementare tutte le misure tecniche e organizzative richieste.

Occorre dunque lavorare su almeno quattro filoni e ci si aspetta che il decreto legislativo di recepimento ne tenga conto.

1. Serve una mentalità risk-driven; un approccio che fondato sulla valutazione, misurazione e trattamento del rischio definisca degli obiettivi di sicurezza piuttosto che misure “minime” (obbligatorie) di sicurezza. L’analisi deve poter essere contestualizzata in un determinato periodo, definendo livelli di sicurezza incrementali e un sistema di controlli mitigativi da adottare in corso d’opera.

2. Il piano delle attività potrà (dovrà) essere notificato all’Autorità in modo che possa essere svolta anche la conseguente attività di vigilanza e ispezione e all’operatore sia lasciata la facoltà di organizzare il proprio lavoro in autonomia e rispettando lo stato iniziale dell’impresa (lo status quo, il T0 delle attività)

3. Il decreto legislativo dovrebbe inoltre mantenere i requisiti di attualità imposti dalla transizione digitale, ovvero una norma con principi di diritto ma che lasci il compito all’autorità di settore di specificare le misure tecniche che possono cambiare nel tempo (e che ahimè cambiano ad una velocità pazzesca!)

4. E’ necessaria una formulazione che renda poi il fornitore, ovvero le terze parti, assoggettato di default agli obblighi di legge, e non sulla base dei contratti con i soggetti interessati, per evitare disparità di trattamento tra supplier designati essenziali/importanti e supplier che potrebbero non esserlo.

In tale quadro come Associazione abbiamo richiesto una consultazione pubblica proprio per dare la possibilità al Parlamento di conoscere preoccupazioni, opportunità e proposte da parte del mercato.

È importante permettere all’economia italiana di crescere gradualmente affinché sia più forte e anche appetibile a interlocutori solidi e credibili, il rischio altrimenti sarà – in controtendenza rispetto alla finalità della norma – di appesantire le nostre PMI rendendo il Paese ancora più debole e dunque una preda più facile di investitori pirata.

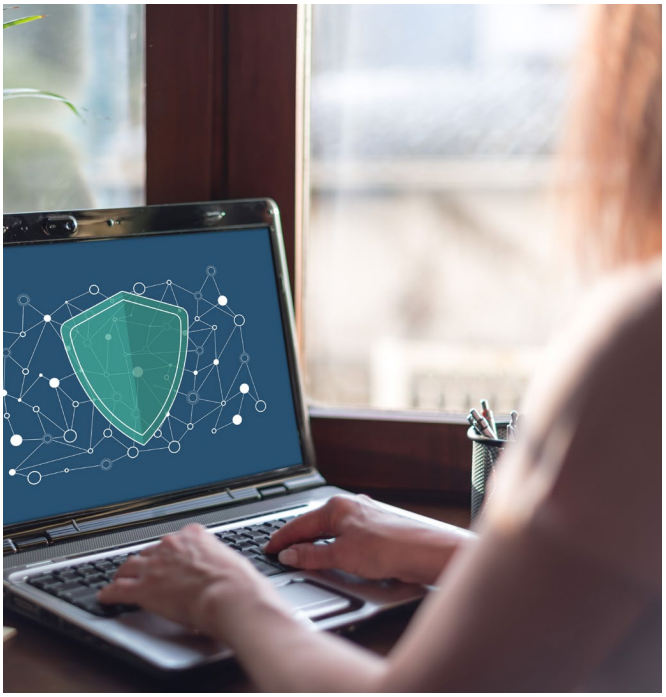
Menti sotto assedio: la rivoluzione umana nella cybersecurity

A cura di Petra Chiste

Con la crescente sofisticazione degli attacchi informatici, che sfruttano non solo le vulnerabilità dei nostri sistemi ma anche quelle insite nella natura umana, come pensi che la psicologia possa arricchire le strategie di sicurezza informatica? È possibile che la chiave per un futuro digitale più sicuro risieda non solo nello sviluppo di tecnologie avanzate, ma anche in una più profonda comprensione dell'elemento umano?

Questo articolo solleva il sipario su una nuova scena in cui la cybersecurity incontra la psicologia umana. Gli attacchi informatici non sono più solo una questione di codici malevoli, si trasformano in narrazioni che giocano sulle nostre vulnerabilità psicologiche. Quindi, quanto è importante, secondo te, che le difese informatiche si evolvano per diventare non solo tecnicamente robuste ma anche psicologicamente intuitive?

Questo dialogo ci spinge oltre i confini tradizionali della cybersecurity, per indagare come una comprensione psicologica possa elevare la nostra resilienza contro le minacce digitali. Riflettendo sul fatto che ogni linea di codice è scritta, ogni clic è eseguito, e ogni trappola è elusa o subita da un individuo, come credi che la nostra percezione della sicurezza informatica debba cambiare?



All'interno dell'ecosistema ICT, l'architettura di sicurezza è rappresentata genericamente da soluzioni tecnologiche. Rappresentano la nostra prima linea di difesa contro le minacce esterne, proteggendo l'accessibilità e l'integrità dei nostri sistemi.

Tuttavia, un elemento critico spesso trascurato in questo schieramento tecnologico è l'aspetto umano. Il phishing, la BEC fraud (Business Email Compromise), sono tecniche che fanno leva esclusivamente sulla componente umana. La loro pericolosità risiede nella sua capacità di apparire convincente, spesso tramite l'utilizzo di messaggi che invocano urgenza o autorità per spingere l'azione precipitosa dell'utente.

Questi attacchi, radicati nell'ingegneria sociale, puntano dritto alle nostre inclinazioni psicologiche — fiducia, paura, sottomissione all'autorità — sottolineando la necessità di un approccio alla sicurezza che superi la pura tecnologia.

Immaginiamo di essere al lavoro, circondati da tutte le tecnologie e le misure di sicurezza più avanzate che il nostro reparto IT possa fornirci. Sembra tutto sotto controllo, giusto? Eppure, basta un momento di distrazione – un clic troppo veloce su un'e-mail che sembrava provenire dal nostro capo, ma che in realtà nascondeva un tentativo di phishing – per mettere a rischio l'intero sistema. È successo a molti, anche ai migliori. Oppure, consideriamo il fenomeno del social engineering, dove gli attaccanti giocano proprio sulla nostra fiducia e sulle nostre abitudini quotidiane. Quante volte abbiamo ricevuto richieste di riconferma delle credenziali o inviti ad accedere a un link per una presunta verifica? Un esempio lampante è quello delle false comunicazioni da parte di fornitori di servizi internet, che invitano ad aggiornare i dati di accesso attraverso link che portano a pagine fasulle. Ma da cosa dipende il successo di questi tentativi?

La percezione del rischio da parte degli individui gioca un ruolo significativo nelle scelte che le persone fanno, influenzando così la strategia di sicurezza a tutti i livelli.

La percezione del rischio non è un'entità statica o uniforme; varia ampiamente tra gli individui, influenzata da un mosaico di fattori psicologici, emotivi, sociali e culturali. Elementi quali esperienze personali, emozioni pre-

valenti, esposizione mediatica e pressioni del contesto sociale si intrecciano per formare un quadro personale del rischio che può differire notevolmente dalla realtà oggettiva. Uno degli aspetti più intriganti di questa percezione è il ruolo dell'esperienza diretta e della narrazione mediatica. Le persone che hanno vissuto eventi negativi o sono state esposte a racconti di tali eventi attraverso i media tendono a sovrastimare la probabilità e la gravità di rischi simili. Questo fenomeno è amplificato dall'effetto dei social media, che possono creare ecosistemi di eco in cui certe percezioni del rischio vengono rinforzate a discapito di una comprensione più equilibrata. La "distanza psicologica" da un pericolo gioca anche un ruolo chiave. Le minacce percepite come prossime, sia in termini temporali che geografici o emotivi, sono spesso valutate come più pressanti e gravi. Questo meccanismo psicologico spiega perché alcune persone possono apparire irragionevolmente preoccupate per rischi immediati, trascurando minacce future o meno visibili che potrebbero, ad un'analisi più attenta, presentare un pericolo maggiore.

La comprensione delle dinamiche della percezione del rischio non è solo di interesse accademico; ha implicazioni concrete per la progettazione di politiche di sicurezza e per l'efficacia delle strategie di gestione del rischio. Nel settore della sicurezza informatica, ad esempio, riconoscere che gli utenti possono avere percezioni distorte dei rischi può aiutare a sviluppare formazioni, comunicazioni e protocolli più efficaci, che tengano conto di questi bias cognitivi e emotivi.

I bias cognitivi ed emotivi sono diversi, vediamo quelli che maggiormente impattano le scelte in ambiti di sicurezza informatica.

La percezione del rischio da parte degli individui gioca un ruolo significativo nelle scelte che le persone fanno, influenzando così la strategia di sicurezza a tutti i livelli.

L'euristica della disponibilità illustra come tendiamo a sovrastimare la probabilità di eventi che possiamo facilmente richiamare alla mente, come attacchi informatici di alto profilo. Questo meccanismo è radicato nella nostra propensione a lasciare che le esperienze recenti, o eccezionalmente vivide, influenzino la nostra percezione della frequenza di eventi simili. È evidente nel modo in cui gli attacchi informatici di alto profilo, come il famigerato WannaCry ransomware, rimangono impressi nella mente degli esperti ICT. Questi eventi creano un punto di riferimento che tende a sovrastimare la probabilità di attacchi simili nel futuro, portando a volte a misure di sicurezza sproporzionate rispetto ad altre minacce meno mediatiche ma potenzialmente più dannose.

L'euristica dell'ancoraggio, d'altra parte, descrive la tendenza a fare affidamento eccessivamente sulle prime informazioni che riceviamo su un argomento, utilizzandole come "ancora" per le valutazioni successive, anche quando si dispone di nuove informazioni. Concentrandosi troppo su un singolo esempio o tipologia di attacco, gli utenti possono diventare meno attenti ad altre forme di minacce che non corrispondono esattamente a quello che hanno imparato o ricordano (ancora).

Il bias di conferma, infine, evidenzia la nostra tendenza a cercare, interpretare e ricordare le informazioni in modo che confermino le nostre preconcezioni, ignorando quelle che le contraddicono. Questo può portare a una visione ristretta dei rischi informatici, dove gli esperti potrebbero non valutare adeguatamente le minacce emergenti o sottovalutare quelle che non si allineano con le loro aspettative esistenti. Un esempio semplice è quando un analista cyber ignora segnali di una violazione dati perché in passato falsi allarmi hanno generato inutili allarmismi.

L'ottimismo irrealistico si manifesta quando gli individui credono che le probabilità di esperienze negative siano minori per loro rispetto agli altri. Negli ambienti ICT, questo può tradursi in una sottovalutazione dei rischi personali o organizzativi e in un falso senso di sicurezza, che potrebbe ostacolare l'adozione di misure preventive efficaci. L'esempio più efficace è l'automobilista che si crede immune dagli incidenti stradali poiché è esperto, sottovalutando tutta una serie di alert o di segnali che possono provenire dall'ambiente in cui si trovano.

La sfida è duplice: da un lato, è necessario informare e formare gli individui per affinare la loro capacità di

valutazione dei rischi, fornendo loro gli strumenti per distinguere tra minacce reali e percepite. Dall'altro, le organizzazioni devono lavorare per creare culture della sicurezza che promuovano una discussione aperta e informata sui rischi, incoraggiando una valutazione più equilibrata che possa guidare verso decisioni più ponderate e strategie di sicurezza più resilienti.

Cominciamo quindi a comprendere come la componente psicologica nella percezione del rischio in sicurezza informatica possa influenzare direttamente i comportamenti specifici degli utenti. Il passo successivo è, quindi, integrare queste conoscenze nella progettazione delle formazioni.

Le formazioni individuate devono da un lato accrescere le conoscenze di sicurezza informatica e dall'altra riconoscere quando ci troviamo di fronte ad un bias.

Consideriamo il caso del phishing, una delle minacce più pervasive e insidiose. Un utente riceve una email che sembra provenire da un fornitore di servizi noto, invitandolo a cliccare su un link per risolvere un problema urgente con il suo account. Qui, l'euristica della disponibilità può portare l'utente a ricordare le volte in cui ha ricevuto comunicazioni legittime simili, sottovalutando i segnali di pericolo che indicano un tentativo di phishing. L'assenza di una valutazione critica, dovuta a un bias di conferma (cerca conferme del suo presupposto che la mail sia genuina), può facilmente tradursi in un clic fatale. Per contrastare gli effetti dei bias cognitivi, è fondamentale esporre i nostri utenti alle più svariate situazioni, in modo tale che possono sviluppare un'euristica più affidabile per valutare le situazioni potenzialmente pericolose, rafforzando le capacità di riconoscimento dei tentativi di phishing o di altre minacce.

Al di là della formazione individuale, è sempre più cruciale promuovere una cultura organizzativa che valorizzi la sicurezza come responsabilità condivisa, incoraggiare la segnalazione proattiva di email sospette o di comportamenti anomali, senza timore di ripercussioni. In questo modo, si coltiva un ambiente in cui le decisioni di sicurezza sono supportate da un contesto sociale che rinforza comportamenti sicuri, piuttosto che affidarsi unicamente al giudizio individuale, spesso soggetto a bias.

Mentre ci avviciniamo alla conclusione di questo articolo emerge una visione chiara: il cammino verso una maggiore sicurezza non è soltanto tecnologico, ma intrinsecamente umano.

La consapevolezza e la comprensione dei bias cognitivi ci offrono una lente attraverso la quale possiamo non solo riconoscere le nostre vulnerabilità ma anche mobilitare le nostre risorse più potenti: la capacità di apprendere, adattarsi e supportarci a vicenda.

L'errore umano non deve essere visto come un punto di fallimento ma, piuttosto, come un punto di partenza per lo sviluppo di strategie di sicurezza più efficaci, inclusive e resilienti.

Il cammino verso una maggiore sicurezza non è soltanto tecnologico, ma intrinsecamente umano.

CYBER
Think Tank
ASSINTEL

Assintel Cyber Hub

Connettiti alla rete della sicurezza!

Obiettivo:

Mappare ed elencare le Aziende associate ad Assintel con competenze in ambito Cyber.

Progetto:

L'Assintel Cyber Hub è un Catalogo Annuale (verrà valutato nel corso dell'anno una differente cadenza di aggiornamento).

Per info scrivi a:

segreteria@assintel.it

Cybersecurity: necessario innovare davvero prima che diventi il tallone d'Achille dell'Italia

A cura di Pierluigi Paganini

La nostra società, sempre più intrisa di tecnologia, si scopre giorno dopo giorno più vulnerabile alle minacce cibernetiche. Ad essere minacciate non sono solo aziende, governi e utenti, nelle ultime settimane abbiamo constatato quanto sia vulnerabile il 'sistema linfatico' del sistema informatico globale. Cavi sottomarini, reti satellitari, sistemi GPS sono sotto attacco da parte dei medesimi attori che sino ad oggi si sono distinti in attacchi cibernetici estremamente sofisticati.

Questa premessa è necessaria per comprende che l'analisi dell'attuale panorama delle minacce necessita di un approccio olistico, che contempli molteplici fattori come la l'evoluzione tecnologica, il contesto geopolitico, livello di digitalizzazione delle nostre infrastrutture, e persino del cambiamento climatico.

L'attuale scenario delle minacce informatiche è caratterizzato da una crescita importante degli attacchi su scala globale, ma continua a preoccupare l'accresciuta complessità.

Desta particolare preoccupazione l'aumentata incidenza degli attacchi sul nostro paese.

Secondo l'ultimo rapporto Clusit, mentre gli attacchi nel 2023 sono aumentati dell'11% a livello globale, in Italia si è registrato un aumento del 65%.

Sempre secondo il rapporto nel 2023, gli attacchi che hanno avuto successo e classificati come "critici" o "gravi" rappresentano ormai oltre l'81% del totale, rispetto al 47% osservato nel 2019.

Il crimine informatico è responsabile per la maggioranza degli attacchi da molti anni (oltre l'80% nel 2023), a seguire attacchi con una motivazione politica e riconducibili, pertanto, ad attori nation-state ed hackvitisti.

Risultati altrettanto allarmanti emergono dal primo Rapporto annuale sull'evoluzione della cybersecurity redatto

dal Cyber Think Tank di Assintel.

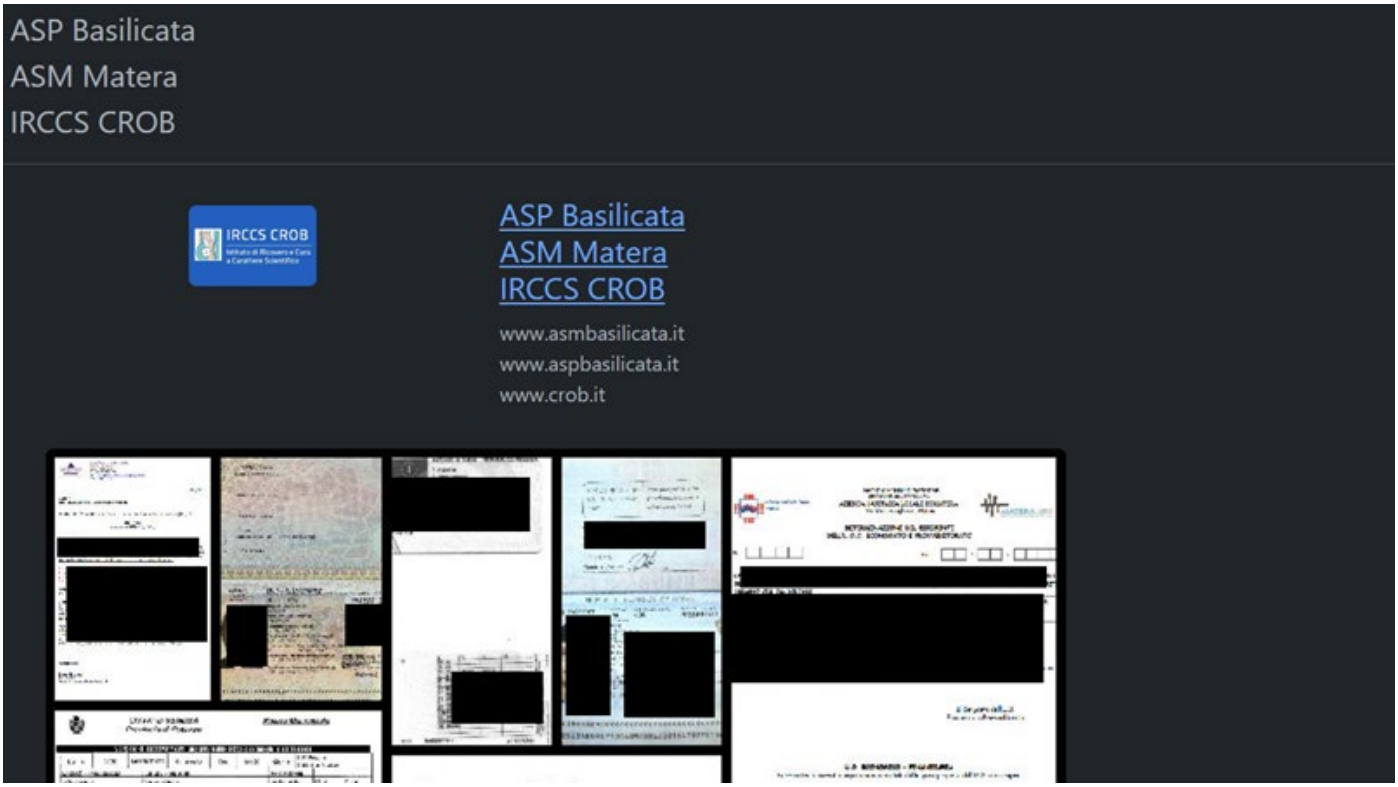
Secondo il rapporto, in Italia, nel primo semestre del 2023 si è registrato un aumento del 85,7% di attacchi rispetto al trimestre precedente. Le PMI risultano le aziende più esposte alle minacce informatiche, un dato che deve indurre ad una riflessione sulla vulnerabilità del tessuto imprenditoriale italiano. Sempre secondo il rapporto Assintel, i settori più colpiti includono manifatturiero, servizi, costruzioni, finanza e sanità.

I malware continuano a rappresentare la principale minaccia alle infrastrutture informatiche di aziende private e pubblica amministrazione. Secondo l'azienda di sicurezza Trend Micro, anche nel 2023, l'Italia è stato il primo Paese europeo e il quarto al mondo per numero di attacchi malware. Preoccupa il fatto che l'Italia occupa le medesime posizioni da oramai tre anni preceduta nel mondo, solo da Giappone, Stati Uniti e India.

Per comprendere la dimensione della minaccia basti sapere che la sola Trend Micro ha intercettato in Italia nel 2023 circa 277.616.731 malware.

Non passa settimana che non apprendiamo di attacchi ransomware od organizzazioni italiane. Purtroppo, questi attacchi hanno un impatto devastante sui cittadini e spesso non ricevono dalla stampa il dovuto risalto.

Questo è il caso dell'attacco all'ASP Basilicata perpetrato dal gruppo ransomware Rhysida che ha rubato dall'azienda sanitari circa in terabyte di dati sensibili comprensivi di cartelle sanitarie e documenti di ignari pazienti, molti dei quali sottoposti a cure oncologiche.



Tor Leak Site Gruppo Rhysida con annuncio attacco all'ASP Basilicata

I malware continuano a rappresentare la principale minaccia alle infrastrutture informatiche di aziende private e pubblica amministrazione.

È lecito chiedersi quale siano le ragioni dietro gli allarmati dati relativi agli attacchi contro l'Italia. Per quale motivo l'Italia è così esposta alle minacce informatiche.

Gli aspetti sono molteplici, ma sicuramente alcuni tra essi possono aiutare la comprensione del fenomeno illustrato. Innanzitutto, occorre tener presente che il tessuto economico del nostro paese è composto principalmente da piccole e medie imprese, realtà che sono evidentemente più vulnerabili alle minacce a causa della scarsa consapevolezza delle minacce informatiche e della mancanza di fondi adeguati ad investimenti in soluzioni e processi necessarie ad aumentare la resilienza delle aziende.

Altro aspetto da considerare è che l'Italia e le sue organizzazioni sono di interesse strategico per molteplici attori nation-state. L'appartenenza alla NATO, così come le relazioni commerciali e diplomatiche con molti paesi asiatici e africani espongono le organizzazioni del nostro Paese a numerose campagne di spionaggio.

Eventi come il conflitto tra Russia e Ucraina e quello tra Israele e Hamas hanno inevitabilmente portato una minaccia supplementare da parte di attor statuali interessati a comprende la postura diplomatica del nostro governo ed a punire con atti di sabotaggio le nostre organizzazioni per il supporto dichiarato all'Ucraina. L'allarme è stato anche lanciato nella relazione annuale dei nostri servizi di intelligence che mette in guarda dal crescente numero di operazioni ibride che potrebbero colpire il nostro paese.

Le minacce informatiche possono avere un impatto significativo sulla vita quotidiana di cittadini, aziende e governi.

Interruzioni di servizi essenziali come l'energia elettrica, acqua e trasporti e l'erosione della fiducia nelle istituzioni e disordini sociali alimentati dalla disinformazione e propaganda online, minacciano la coesione sociale e la stabilità politica dei paesi

Minare dall'interno l'Alleanza Atlantica e favorire correnti politiche vicine a Mosca è un obiettivo perseguibile attraverso la disinformazione, il cui potere è amplificato da tecnologie come l'intelligenza artificiale generativa.

Le principali tendenze emergenti che potrebbero avere un impatto significativo sulla sicurezza cyber nel futuro sono sicuramente l'incremento degli attacchi alle catene di fornitura, l'evoluzione del modello "as-a-service", ma soprattutto l'intelligenza artificiale (IA).

L'IA ha un impatto importante sulle nostre vite, così come sulla sicurezza informatica. La sua capacità di automatizzare processi complessi e di analizzare grandi volumi di dati la rende uno strumento prezioso per la difesa contro le minacce informatiche. Tuttavia, l'IA può essere utilizzata anche dagli attaccanti per condurre attacchi sofisticati quali come deepfake e spear-phishing. L'intelligenza artificiale potrebbe essere impiegata per automatizzare i processi ricognitivi negli attacchi per l'individuazione di falle oppure per eludere i classificatori utilizzati dai sistemi in difesa.

Per contrastare le minacce legate all'IA, è fondamentale investire nella ricerca e nello sviluppo di tecnologie di sicurezza basate sull'IA. Sebbene si annuncino investimenti importanti, occorre tener presente che aziende private come Meta investiranno in ricerca su IA da sole decine di miliardi di dollari nel 2024. Una singola azienda privata americana investirà oltre dieci volte la cifra stanziata dal nostro governo per la ricerca nazionale in materia, e l'Italia in questo momento si distingue in Europa per quest'impegno.

È cruciale essere consapevoli dei rischi e delle opportunità associate all'IA per poter promuovere un utilizzo responsabile e sicuro e prevenire ogni abuso.

Il futuro della cyber sicurezza è sicuramente legato alla capacità di sviluppare difese intelligenti ed in grado di adattarsi e rispondere in tempo reale alle nuove minacce.

Dobbiamo imparare ad innovare lasciandoci alle spalle modelli di difesa cibernetica sempre meno efficaci, in gioco vi è la sovranità nazionale e le libertà che, come individui, abbiamo conquistato con secoli di lotte.

L’utilizzo dell’IA nella cybersecurity

A cura di Paolo Montali

Il panorama delle minacce informatiche continua a svilupparsi in modo iperbolico e lo vediamo dai report che ci arrivano da tutti i centri studi della cyber criminalità. Gli autori delle minacce utilizzano vettori e metodologie di attacco sempre più sofisticati e le organizzazioni che lottano per proteggersi sono sempre in affanno, soprattutto con i rischi introdotti dall’utilizzo di infrastrutture multi-cloud ibride e con il lavoro da remoto o ibrido. In questo periodo dove il panorama socioeconomico globale rimane instabile, vediamo di esaminare la situazione.

È evidente che i criminali informatici traggono già oggi un significativo vantaggio dall’utilizzo dell’ intelligenza artificiale (IA), per aumentare le probabilità di successo in una vasta gamma di attività malevole. In particolare negli attacchi DDoS (Distributed Denial of Service), i sistemi esperti sono in grado di ottimizzare i vettori di attacco implementati dagli autori delle minacce, svolgendo attività di scansioni e risultati dei test delle prestazioni in tempo reale, sono già diventati più diffusi.

L’intelligenza artificiale sta emergendo sempre di più, e la tecnologia è già utilizzata in molti modi diversi. Ad esempio, l’intelligenza artificiale viene utilizzata per accelerare e ottimizzare le azioni dell’intelligence effettuate da chi si difende, sulle minacce. Oggi questa tecnica fornisce già dei risultati interessanti molto più rapidamente e con maggiore efficacia rispetto al passato, aiutando le organizzazioni a difendersi meglio. L’intelligenza artificiale generativa viene utilizzata per fornire assistenza in linguaggio naturale durante l’analisi delle minacce, aiutando le organizzazioni a massimizzare l’efficacia dell’attività di analisi nei loro SOC. Oltre a ciò, viene utilizzata un’intelligenza artificiale più “tradizionale” per aiutare a identificare anomalie che altrimenti passerebbero inosservate, come ad esempio l’ormai consolidata azione di controllo delle abitudini di comportamento dell’utente. Si prevede che tutto questo continuerà, con risultati che miglioreranno ulteriormente man mano che tutti impareremo di più da questa tecnologia emergente.

Bisogna prestare una certa attenzione nell’utilizzo dell’IA perché questa nuova tecnologia deve ancora subire diversi passaggi per renderla stabile e completamente affidabile e comunque il vecchio “adagio IT” che dice “se prendi in input dati spazzatura, non potrai che avere dati spazzatura in output”’ è ancora valido. Se inserisci dati scarsi, probabilmente otterrai scarsi risultati, indipendentemente da quanto sofisticati siano i tuoi algoritmi. A tal fine, laddove i clienti desiderano utilizzare l’intelligenza artificiale, sia per la sicurezza che per le attività operative, per il marketing o per altri campi di applicazione, se deve mettere una sempre maggiore attenzione nella fase di acquisizione dei set di dati, per garantirsi un livello qualitativo per bilanciare l’efficienza e il volume di dati raccolti ed archiviati con un livello di fedeltà e accuratezza adeguato per ottenere i migliori risultati dall’investimento nell’intelligenza artificiale.

Le Best Practice per una più ampia difesa informatica

È fondamentale che tutte le aziende dispongano di una strategia di sicurezza a tutto tondo, sufficientemente ampia da coprire l'identificazione e la qualificazione, in modo proattivo, dei rischi. Questo concetto è valido sia per l'ambito informatico e delle telecomunicazioni sia per tutte le attività delle Aziende. Per quanto riguarda l'ambito cyber passa attraverso la selezione delle tecnologie, l'approvvigionamento e l'utilizzo dell'intelligence. È inoltre fondamentale che le tecnologie di sicurezza utilizzate forniscano una visibilità coerente in tutta l'azienda, eliminando i punti ciechi interni o esterni e facilitando l'attività di rilevamento, indagine, correzione, analisi forense e di reporting che sia coerente con gli obiettivi di sicurezza che l'Azienda si è posta. In aggiunta a ciò, l'intero ecosistema dovrebbe essere il più integrato possibile per ridurre le spese generali operative e accelerare la risposta alle minacce.

Tutto ciò però non deve portare ad una estremizzazione sulla governance della sicurezza informatica, ma deve portare a piani strutturati e delineati in modo chiaro con obiettivi precisi e con delle fasi di verifica e controllo periodici. Queste attività devono essere studiate sulla base dell'analisi dei rischi effettuata e sulla base delle capacità economiche dell'azienda. Bisogna comunque ricordare che un buon piano di sicurezza informatica dovrebbe essere testato trimestralmente - o nel peggiore dei casi ogni semestre per mantenerlo aggiornato alle crescenti minacce e per creare quella familiarità a questi aspetti che non è ancora così entrata nel tessuto e nella prassi delle Aziende che spesso vedono questo aspetto come una punta di un iceberg di cui non conoscono molto bene i confini.

In ultimo, ma non meno importante, dobbiamo coinvolgere nel viaggio verso una maggiore sicurezza non solo l'area tecnica IT, ma tutti i membri dell'azienda, ognuno con il suo ruolo e il suo compito, ma ciascuno di noi può essere un piccolo tassello, ma fondamentale per rafforzare il sistema di sicurezza Aziendale. Tutti devono capire che hanno un ruolo da svolgere nella protezione dei dati e dei processi della propria organizzazione. Ciò significa che i dipendenti devono effettivamente prendere in considerazione il fatto che la mancata applicazione delle politiche e delle migliori pratiche, anche quelle piccole scorciatoie che ci concediamo pensando ."ma si dai! Ma non succede niente…." potrebbe avere un impatto significativo sull'azienda nel suo complesso, oltreché sulla carriera delle persone.

Questo vuol dire un approccio al tema della sicurezza informatica che va oltre il semplice partecipare ad una serie di corsi di formazione obbligatori sulla sicurezza - questa è una questione di cultura - si tratta di integrare i messaggi di sicurezza nelle comunicazioni della leadership, nel reporting aziendale e in ogni altro aspetto dell'attività aziendale quotidiana, quindi che la sicurezza è sempre una considerazione che ci troviamo in tutti gli ambiti, dall'ufficio, al rapporto con i fornitori e con i clienti, a casa o anche quando siamo in ferie.

CYBER
Think Tank
ASSINTEL

Il brand “Made in Italy” nel settore agroalimentare: un volano per l’economia Italiana

A cura di Marco Porcedda

Al giorno d’oggi, il “Made in Italy” rappresenta un vero e proprio emblema di eccellenza nel settore agroalimentare, riconosciuto e celebrato su scala globale. Questo prestigio non solo evidenzia la qualità e l’unicità dei prodotti italiani, ma si traduce anche in un contributo economico significativo per il Paese. L’agroalimentare gioca ormai un ruolo chiave nell’economia italiana, contribuendo in modo sostanziale al Prodotto Interno Lordo (nel 2023 la produzione totale della filiera agroalimentare italiana, tra produzione, trasformazione, distribuzione e ristorazione, ha toccato i 550 miliardi di euro, pari al 15% del PIL) e rappresentando una delle principali voci nel paniere nazionale.

Negli ultimi anni, il settore ha visto, in particolare, una crescita costante dell’export, con un notevole incremento del valore dei prodotti italiani sui mercati internazionali (+6% nel solo 2023, superando per la prima volta nella storia la cifra di 64 miliardi di euro). Il trend positivo è un sicuro e diretto riflesso della capacità delle aziende italiane di coniugare sapientemente tradizione e innovazione, offrendo prodotti che rispondono alle esigenze di qualità, sicurezza e sostenibilità richieste dai consumatori globali. La valorizzazione del Made in Italy passa anche attraverso la tutela della sua autenticità e la lotta alla contraffazione, sfide che vedono anche nella tecnologia un potente alleato.

Tuttavia, la crescente esposizione sui mercati esteri ed il valore di quello che ormai è diventato a tutti gli effetti un brand, espone il settore a nuovi rischi, ulteriori rispetto alla “semplice” contraffazione, tra cui quelli legati alla cybersecurity e alla necessità di garantire la protezione dei dati e la tracciabilità dei prodotti in un settore produttivo sempre più digitalizzato ed iperconnesso. In questo contesto, il Made in Italy non solo deve difendere la sua eredità di qualità e tradizione, ma deve anche districarsi tra le complessità del commercio internazionale moderno, affrontando con determinazione le sfide poste dalla digitalizzazione e dall’innovazione tecnologica.

Tracciabilità e lotta alla contraffazione: la tecnologia Blockchain come soluzione innovativa per tutelare la brand reputation

In risposta alle sfide poste dalla contraffazione e dalla necessità di garantire una tracciabilità sempre più efficace ed accessibile dei prodotti agroalimentari, la tecnologia blockchain si è rivelata una soluzione all’avanguardia perfettamente adeguata a rispondere alle specifiche necessità del settore. Questa tecnologia, conosciuta inizialmente per il suo utilizzo nella produzione di criptovalute, offre un sistema di registrazione dati pubblico, decentralizzato, immutabile e trasparente, ideale per la tracciabilità dalla produzione al consumatore finale.

La blockchain offre una risposta concreta al bisogno di trasparenza e sicurezza, permettendo di registrare ogni passaggio del prodotto all’interno della filiera in un “libro mastro” digitale, accessibile da chiunque in maniera open-source, ma non modificabile se non attraverso particolari procedure, comunque tracciate, intervenendo sulla struttura stessa della catena. Questo assicura che tutte le informazioni relative alla produzione, trasporto, trasformazione e distribuzione dei beni siano verificabili ed inalterabili, contrastando efficacemente la contraffazione e fornendo al consumatore una maggiore garanzia sulla genuinità del prodotto acquistato.

L’impiego della blockchain nel settore agroalimentare italiano non solo rafforza la lotta alla contraffazione ma contribuisce significativamente alla tutela della brand reputation del “Made in Italy”. Già dal 2017 aziende pionieristiche in questo campo hanno dimostrato come l’adozione di questa tecnologia potesse migliorare la fiducia dei consumatori nei prodotti italiani, aumentando così il loro valore sia sul mercato nazionale che internazionale. A distanza di anni, l’utilizzo di questa tecnologia per la tracciabilità nel settore agroalimentare ha subito una notevole accelerazione, anche grazie a realtà produttive ad elevato tasso tecnologico che ben si sposano con processi automatizzati propri dell’industria 4.0.

Inoltre, la capacità della blockchain di fornire una tracciabilità dettagliata e affidabile si rivela fondamentale in situazioni di crisi, permettendo una rapida identificazione ed isolamento dei lotti che possono risultare fonte di problemi legati alla sicurezza alimentare. Questo non solo contribuisce a salvaguardare la salute dei consumatori, ma protegge anche l’immagine delle aziende e dell’intero settore agroalimentare italiano, arginando il mancato fatturato dovuto al blocco totale di quella produzione e prevenendo potenziali danni alla reputazione causati da eventi negativi.

Protezione dei dati e sicurezza della blockchain per la tutela del Made in Italy nell'agroalimentare italiano

Non bisogna dimenticare, però, che in un'era caratterizzata da una digitalizzazione intensiva, la protezione dei dati e la sicurezza delle informazioni rappresentano pilastri fondamentali anche per l'industria agroalimentare italiana, sempre più caratterizzata da un elevato tasso di automazione ed informatizzazione, che la espone quindi a rischi più estesi. Il settore si trova a dover difendere il proprio patrimonio anche dalle incursioni di cybercriminali sempre più sofisticati. La blockchain emerge come una soluzione d'avanguardia, offrendo un meccanismo di sicurezza robusto, che garantisce l'integrità e la confidenzialità delle informazioni senza compromettere l'accessibilità.

Questo sistema di registrazione distribuito assicura che ogni transazione, ogni cambio di stato e ogni dato inserito nella catena siano permanenti e inalterabili. La decentralizzazione intrinseca della tecnologia riduce il rischio di attacchi informatici mirati, poiché non esiste un unico punto di fallimento che possa essere sfruttato per compromettere l'intero sistema. Implementare questa tecnologia significherebbe, quindi, elevare ulteriormente gli standard di sicurezza ed affidabilità del Made in Italy, proteggendo le aziende da possibili danni reputazionali e finanziari dovuti a frodi o adulterazioni. Inoltre, la capacità di assicurare la provenienza autentica dei prodotti rafforzerebbe la fiducia dei consumatori, elemento chiave per il posizionamento competitivo dei prodotti italiani sui mercati internazionali. Si tradurrebbe, in fondo, in una ulteriore evoluzione dell'originario concetto dei Consorzi di Tutela, che avrebbero essi stessi uno strumento più efficace di controllo ed intervento.

Rischi ed opportunità tecnologiche per il settore agroalimentare

Investire nella blockchain potrebbe quindi rappresentare una strategia vincente per le aziende del settore, che potrebbero così garantire l'autenticità dei loro prodotti, difendere il valore del brand "Made in Italy" e consolidare la loro posizione nei mercati globali. La sfida è quella di estendere l'utilizzo di questa tecnologia su scala più ampia, promuovendo standard comuni e collaborazioni tra imprese, istituzioni e organizzazioni a carattere tecnologico, per una protezione efficace e innovativa del patrimonio agroalimentare italiano intervenendo in primis sugli standard che disciplinano la produzione "100% italiana" o "Made in Italy".

Non bisogna però idolatrare l'evoluzione tecnologica fine a se stessa e occorre tenere sempre presente che ogni strumento tecnologico, dalla blockchain agli algoritmi LLM o GPT – la cosiddetta "Intelligenza Artificiale" – presenta sia opportunità che rischi significativi, influenzando direttamente la crescita economica del Paese. Da un lato, la digitalizzazione e l'adozione di tecnologie avanzate, come la blockchain ed il machine learning, offrono strumenti potenti per la tracciabilità dei prodotti, la gestione efficiente della filiera e la lotta alla contraffazione, rafforzando la brand reputation del Made in Italy; d'altro canto, l'aumento della dipendenza da sistemi digitali espone il settore a rischi cyber sempre più sofisticati, richiedendo consapevolezza, attenzione ed investimenti continui in sicurezza informatica. Questo scenario sottolinea la necessità di un equilibrio tra innovazione, sicurezza e legislazione, dove le opportunità di crescita economica e di espansione sui mercati internazionali devono essere perseguite con una consapevole gestione dei rischi ed una equilibrata lungimiranza.

Cyber per tutti

Istruzioni semplici per questioni complesse!

CYBER Think Tank ASSINTEL

Per info scrivi a:
segreteria@assintel.it

Cyber Think Tank Assintel

Il cert finanziario italiano (CERTFin): rafforzare la cyber resilience di settore attraverso la cooperazione pubblico-privata

A cura di Mario Trinchera

In tutto il mondo le minacce alla cybersecurity, e di conseguenza le realtà e le soluzioni per contrastarle, sono in forte trasformazione. Cresce l'interoperabilità dei servizi essenziali e aumentano esponenzialmente i dispositivi connessi alle reti.

Partendo da questo dato di fatto, la Direttiva UE 2016/1148 (Direttiva NIS) ha evidenziato la necessità di rafforzare la collaborazione tra i diversi Paesi e tra i diversi settori. Inoltre, a partire dal decreto di recepimento della Direttiva (d.lgs. 18 maggio 2018, n.65), sono in corso di definizione e attuazione diverse misure di potenziamento dell'architettura nazionale di sicurezza informatica. L'intervento normativo più recente è la legge di conversione del decreto Cybersecurity (l. 18 novembre 2018, n.133), che indica "disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica".

In tale contesto il settore finanziario è di fatto particolarmente colpito dagli attacchi di tipo cyber, nonostante l'adozione massiva di soluzioni tecnologiche che svolge un ruolo importante nella difesa delle nostre finanze. In Italia, con l'obiettivo di aumentare la capacità di gestione dei rischi cyber dei diversi operatori, è stato istituito nel 2017 il CERTFin (CERT Finanziario Italiano), che rappresenta oggi un punto di contatto privilegiato del settore finanziario con le Istituzioni competenti per la protezione cibernetica e la sicurezza informatica. Il CERTFin fornisce supporto operativo e strategico alle attività di prevenzione e risposta agli attacchi informatici e agli incidenti di sicurezza.

È un'iniziativa pubblico-privata governata dalla Banca d'Italia e dall'Associazione Bancaria Italiana (ABI) e operata da ABI Lab, il Centro di Ricerca e Innovazione per la Banca promosso dall'ABI in un'ottica di collaborazione tra banche, aziende e Istituzioni. La partecipazione al CERTFin è aperta e su base volontaria e conta ad oggi 68 aderenti (istituti bancari, compagnie assicuratrici, infrastrutture di mercato e centri servizi).

Le attività del CERTFin si dividono in diversi filoni operativi. Tra i principali, vi è lo scambio tempestivo di informazioni tra gli operatori del settore su potenziali minacce informatiche (Financial Info Sharing and Analysis center – FinISAC): il CERTFin seleziona gli indicatori di compromissione relativi a potenziali minacce e gli indicatori di frode di maggiore interesse per il settore finanziario, filtrando le informazioni ricevute da molteplici fonti e condividendole con gli aderenti attraverso una piattaforma open denominata MISP (Malware Info-Sharing Platform). Nell'arco dei sette anni di operatività, il CERTFin ha analizzato migliaia di fenomeni e ha raccolto oltre 50 milioni di indicatori specifici per il settore finanziario.

Un altro ambito di attività consiste in un vero e proprio osservatorio di ricerca (Cyber Knowledge and Security Awareness - CyKSA): rappresenta un'occasione di confronto su diversi argomenti, attraverso incontri periodici partecipati da oltre 100 esperti delle realtà aderenti che si aggiornano su minacce, modelli di attacco, soluzioni tecnologiche ma anche sulle normative di riferimento per il settore. Oltre agli aderenti, all'osservatorio partecipano occasionalmente soggetti esterni di particolare rilievo, per favorire una discussione più approfondita su specifici fenomeni (es. Polizia Postale, Telco Providers, rappresentanti dei circuiti di pagamento internazionali, ecc.).

Il CERTFin svolge anche attività di Threat Intelligence attraverso una propria piattaforma che analizza fonti aperte e chiuse per intercettare tempestivamente le minacce emergenti e approfondirle indipendentemente dal fatto che il loro target sia un'azienda o un cliente. I risultati di queste analisi confluiscono nel report semestrale "Threat Landscape Scenario for the italian financial sector" che fornisce una panoramica sulle principali minacce che il settore dovrà affrontare nei mesi successivi.

Un altro filone di attività riguarda le esercitazioni cyber, organizzate dal CERTFin per consentire ai soggetti aderenti di verificare l'efficacia dei propri processi difensivi. Le esercitazioni sono prevalentemente di tipo Table Top, simulazioni che ripercorrono con ritmi serrati uno scenario ben dettagliato definito in base alle minacce recentemente osservate.

Inoltre, accrescere l'awareness delle persone sui rischi che possono provenire dall'utilizzo dei servizi finanziari attraverso la rete è un'altra priorità del CERTFin, che ha realizzato con successo, fin dal 2019, diverse campagne di sensibilizzazione per il settore. Il CERTFin negli ultimi anni ha promosso campagne di cybersecurity awareness che hanno coinvolto diverse banche e istituzioni (I Navigati, CyberSicuri), unite in uno sforzo comune per rendere ancora più sicure le transazioni online e ridurre l'impatto del "fattore umano" sulle frodi informatiche.

Infine, il CERTFin partecipa a diverse iniziative internazionali, prendendo parte stabilmente a numerosi tavoli di lavoro guidati dalle maggiori realtà europee in materia di sicurezza e protezione dei sistemi di pagamento (Enisa, Europol, FS-ISAC, G7-CEG, EBF CSWG, EPC, Swift, …), ed è coinvolto attivamente in numerosi progetti finanziati dall'Unione Europea.

In conclusione, in un contesto come quello attuale in cui il crimine informatico sta diventando sempre più sofisticato, la capacità di agire in maniera strutturata e coordinata, facendo in modo che la cultura della sicurezza vada oltre i confini delle singole organizzazioni, può costituire un fattore determinante.

CERTFin

In tutto il mondo le minacce alla cybersecurity, e di conseguenza le realtà e le soluzioni per contrastarle, sono in forte trasformazione.

Data breach regione Lazio

A cura di Paola Righetti

Vi ricordate l'attacco informatico alla Regione Lazio nell'agosto del 2021?

A seguito di tale attacco, il Garante della Protezione dei Dati Personali ha avviato un'ispezione, il cui esito è stato comunicato con la newsletter del 10 aprile scorso. In essa il Garante informa che in data 21 Marzo 2024 ha emanato 3 provvedimenti sanzionatori nei confronti rispettivamente di Regione Lazio, LAZIOCrea e la ASL 3 (provv. 10002287, 10002324 e 10002533)

Dai provvedimenti del Garante c'è sempre da imparare, per orientare le interpretazioni sui requisiti del GDPR.

Spesso la certificazione del sistema di gestione per la sicurezza delle informazioni (SGSI) UNI CEI ISO/IEC 27001:2017, viene indicata come una certificazione che mette l'azienda al sicuro dalle sanzioni del Garante per la protezione dei dati, come vedremo non è così e lo testimonia la sanzione di 270.000 euro inflitta al titolare del trattamento: la Regione Lazio.

Nel provvedimento relativo alla Regione Lazio (provv. 10002287), tra le altre cose il garante fornisce la sua interpretazione sul possesso delle certificazioni volontarie relative al Sistema di Gestione per la Sicurezza delle Informazioni (UNI CEI ISO/IEC 27001:2017):

".. con riferimento alle ricorrenti argomentazioni fondate sul possesso, da parte di LAZIOcrea, della certificazione del sistema di gestione per la sicurezza delle informazioni (SGSI) in conformità alla norma UNI CEI EN ISO/IEC 27001:2017, con estensione ai controlli della ISO 27017 e ISO 27018, si evidenzia che tale certificazione non rientra, al momento, tra quelle previste dall'art. 42 del Regolamento.

In ogni caso, la certificazione ai sensi dell'art. 42 del Regolamento, seppur possa essere utilizzata, da titolari o responsabili, come elemento per dimostrare il rispetto degli obblighi del Regolamento, non ne implica automaticamente il rispetto.

Inoltre, occorre considerare che la certificazione di un SGSI può essere limitata a specifici ambiti (servizi e/o sedi) dell'organizzazione (riportati sinteticamente nel certificato rilasciato dall'organismo di certificazione) e che il processo di certificazione di un SGSI, basato principalmente sui risultati degli audit (verifiche documentali e sul campo), contiene elementi di incertezza sia perché legato al concetto di rischio sia perché svolto su un campione dei processi che l'organizzazione, ferma restando la sua buona fede, sottopone a certificazione.

La certificazione di un SGSI basato sulla ISO/IEC 27001, quindi, non garantisce, di per sé, livelli di sicurezza, controlli o misure di sicurezza stabiliti o fissati a priori, ma assicura l'adozione dei controlli che l'organizzazione ha identificato e ritenuto adeguati sulla base di una propria valutazione del rischio.

Il titolare del trattamento, pertanto, quando si avvale di un responsabile del trattamento certificato, secondo meccanismi di certificazione, a prescindere che siano approvati o meno ai sensi dell'art. 42 del Regolamento, dovrebbe sempre verificare se le garanzie offerte dal medesimo responsabile siano efficaci e adeguate ai trattamenti a quest'ultimo affidati".

La Regione Lazio, infatti, durante le ispezioni aveva più volte ribadito, che le misure di sicurezza implementate da LazioCrea erano adeguate perché la società era certificata ISO/IEC 27001.

"..con specifico riferimento alle misure adottate dal responsabile, sulla base delle istruzioni impartite del tito-

lare, al fine di assicurare il rispetto degli obblighi di sicurezza di cui all'art. 32 del Regolamento, resta comunque fermo che il titolare rimane responsabile dell'attuazione di misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al Regolamento, come richiesto dall'art. 24 del medesimo (cfr. punti 37 e 135).

D'altronde, oltre agli imperativi obblighi di vigilanza, le responsabilità in capo al titolare non si esauriscono con la stipula dell'atto giuridico di cui all'art. 28, par. 3, del Regolamento e con la disposizione delle istruzioni relative al trattamento, ma durano per tutto il tempo in cui il responsabile tratta i dati per suo conto. Pertanto, sia il titolare che il responsabile possono essere oggetto di sanzioni in caso di inadempimento degli obblighi stabiliti dal Regolamento poiché entrambi sono direttamente tenuti ad assicurarne il rispetto (cfr. punto 9 delle citate Linee guida)".

Nel caso di specie, il Garante ha considerato che le misure di sicurezza implementate dalla Regione Lazio, per mezzo di LAZIOCrea, non fossero adeguate al rischio, infatti:

"i trattamenti effettuati nel contesto in esame richiedono l'adozione dei più elevati standard di sicurezza al fine di non compromettere la riservatezza, l'integrità e la disponibilità dei dati personali, anche sulla salute, di milioni di interessati assistiti. Ciò, tenendo altresì conto delle finalità dei trattamenti e della natura dei dati personali trattati, appartenenti anche a categorie particolari. Su tale base, gli obblighi di sicurezza imposti dal Regolamento richiedono l'adozione di rigorose misure tecniche e organizzative, includendo, oltre a quelle espressamente individuate dall'art. 32, par. 1, lett. da a) a d), tutte quelle necessarie ad attenuare i rischi che i trattamenti presentano."

In questo scenario, è fondamentale riconoscere che l'essere in possesso di certificazioni come la ISO/IEC 27001 non esonera le organizzazioni dal continuo monitoraggio e aggiornamento delle proprie pratiche di sicurezza.

La vicenda della Regione Lazio ci ricorda l'importanza di un approccio proattivo e responsabile verso la protezione dei dati, in cui la certificazione non è vista solo come un traguardo raggiunto, ma come parte di un processo di miglioramento continuo.

REGIONE LAZIO

Minacce 2030

A cura di Corrado Giustozzi

Nel complesso momento storico in cui stiamo vivendo, nel quale la minaccia cibernetica cresce vertiginosamente, sia in quantità che in qualità, e gli avversari sfruttano sistematicamente ogni nuovo sviluppo tecnologico per condurre attacchi sempre nuovi e sempre più sofisticati, è importante ragionare sulle tendenze evolutive del fenomeno per cercare di anticiparne gli scenari futuri, così da non farci cogliere impreparati da sviluppi imprevisti o inattesi.

A ciò ha pensato ENISA, l'Agenzia dell'Unione europea per la cybersecurity, che già due anni fa aveva svolto un'interessante analisi prospettica presentandone i risultati in un rapporto intitolato "Identifying Emerging Cyber Security Threats and Challenges for 2030" pubblicato a marzo 2023. Recentemente, a marzo 2024, ENISA ha pubblicato una nuova versione del rapporto, aggiornandolo alla luce di tutto ciò che è successo nell'ultimo anno. È quindi interessante andare a vedere quali sono le indicazioni del nuovo rapporto, e gli scenari da esso delineati.

Ricordiamo che ENISA aveva prodotto il suo rapporto precedente analizzando diversi scenari evolutivi, grazie all'adozione di una metodologia sistematica e alla collaborazione di molti esperti internazionali. Il risultato era consistito in una lista ragionata delle dieci principali minacce alla cybersecurity da qui al 2030. Quella "Top Ten", con le minacce elencate in ordine decrescente di pericolosità, era così composta (i nomi sono quelli originali per evitare traduzioni arbitrarie):

1. Supply chain compromise of software dependencies
2. Advanced disinformation campaigns
3. Rise of digital surveillance authoritarianism / loss of privacy
4. Human error and exploited legacy systems within cyber-physical ecosystems
5. Targeted attacks (e.g. ransomware) enhanced by smart device data
6. Lack of analysis and control of space-based infrastructure and objects
7. Rise of advanced hybrid threats making use of different and unforeseen modus operandi (e.g. disinformation)
8. Skill shortage
9. Cross border ICT service providers as a single point of failure
10. Abuse of AI

Come si vede, due anni fa la principale preoccupazione degli esperti si concentrava su uno degli aspetti di rischio collegato alla supply chain, in particolare quello della compromissione delle dipendenze software tra soggetti posti lungo la medesima filiera produttiva. Si tratta infatti di una vulnerabilità sistemica estremamente pericolosa, che può causare effetti devastanti e ad ampio raggio: ed il timore è che in futuro possa essere sfruttata in modo molto più sistematico di quanto non lo sia stata sinora nei relativamente pochi casi noti.

Al secondo posto si trovavano le campagne di disinformazione massive, condotte con tecniche avanzate quali i deep fake e le reti di utenti fittizi sui social network. Data la tendenza delle persone ad informarsi sempre meno su fonti ufficiali, e sempre più tramite le proprie "bolle" personali sulle reti sociali, queste campagne mirate potrebbero facilmente spostare l'opinione pubblica e, ad esempio, condizionare gli esiti di elezioni politiche o orchestrare movimenti popolari.

Guardando invece agli ultimi posti della classifica del rapporto precedente è interessante notare come la carenza di competenze, su cui praticamente tutti gli osservatori puntano il dito come uno dei fattori critici che condizionano in senso negativo lo sviluppo dell'Europa digitale, fosse solo al terz'ultimo posto; e il rischio di abusi nell'utilizzo dell'intelligenza artificiale addirittura all'ultimo.

Il lavoro di revisione condotto da ENISA per produrre l'aggiornamento del rapporto al 2024 è consistito nella rivalutazione di tutti gli scenari di rischio considerati nella precedente analisi, compresi quelli che non erano entrati nella Top Ten, aggiungendovi nuove minacce introdotte nel frattempo dagli esperti alla luce delle evoluzioni più recenti.

Il risultato, pubblicato sotto forma di semplice aggiornamento e non di rapporto completo, ha portato ENISA a stilare una nuova classifica: nella nuova edizione quindi alcune minacce hanno cambiato leggermente nome in funzione di una loro migliore definizione, alcune sono proprio uscite dall'elenco ed altre ne hanno preso il posto. La nuova Top Ten 2024 è dunque la seguente, nella quale le voci in neretto sono quelle che non erano presenti nella precedente versione 2023 (i titoli sono sempre in originale):

1. Supply chain compromise of software dependencies
2. Skill shortage
3. Human error and exploited legacy systems within cyber-physical ecosystems
4. Exploitation of unpatched and out-of-date systems within the overwhelmed cross-sector tech ecosystem
5. Rise of digital surveillance authoritarianism / loss of privacy
6. Cross-border ICT service providers as a single point of failure
7. Advanced disinformation / influence operations (IO) campaigns
8. Rise of advanced hybrid threats
9. Abuse of AI
10. Physical impact of natural/environmental disruptions on critical digital infrastructure

Analizziamo e commentiamo dunque rapidamente questa nuova classifica.

Innanzitutto, come si vede, il tema della compromissione della supply chain rimane saldamente al primo posto, confermandosi come lo scenario più preoccupante da qui alla fine del decennio. Inaspettatamente, invece, balza al secondo posto la carenza di competenze, che viene percepita come sfida cruciale per le sorti della digitalizzazione a tutto tondo. Le vulnerabilità dei sistemi legacy negli ecosistemi cyber-fisici salgono al terzo posto, scalzando il rischio di derive autoritarie nell'uso delle tecnologie di sorveglianza che scende alla quinta posizione.

Il quarto posto è ora occupato dalla prima delle due new entry, che riguarda il rischio costituito dalla presenza, in quegli ecosistemi tecnologici posti trasversalmente a diversi settori industriali, di sistemi obsoleti e non aggiornati/aggiornabili. L'altra riguarda invece l'impatto fisico delle perturbazioni ambientali sulle infrastrutture digitali, comparsa al decimo posto. Provenienti entrambe dalle posizioni fuori classifica dello studio precedente, queste due voci riflettono la crescente consapevolezza sulle vulnerabilità sistemiche associate ai sistemi obsoleti, e sui potenziali "effetti domino" che dal dominio fisico possono riverberarsi su quello cibernetico.

Le due categorie escluse dalla Top Ten di quest'anno riguardano la perdita di controllo su oggetti e infrastrutture del segmento spaziale, e gli attacchi amplificati da dati provenienti da dispositivi "smart": si tratta in entrambi i casi di minacce puntuali e immediate, che come si vede hanno lasciato il posto a rischi di maggior portata e soprattutto multi-dominio.

Da notare infine come la minaccia costituita dalle campagne di disinformazione e influenza sia scesa al settimo posto, dal secondo che occupava l'anno scorso; mentre è interessante notare come il rischio di abuso dell'IA sia ancora in coda, anche se salito di una posizione, nonostante il gran clamore anche mediatico sorto durante l'ultimo anno attorno a tutto ciò che riguarda l'intelligenza artificiale.

L’evoluzione del ruolo della sicurezza cibernetica con l’avvento delle più recenti tecnologie di frontiera

A cura di Paolo Dal Cin

Gli incessanti cambi di passo nella progressione tecnologica quali l’intelligenza artificiale basata su apprendimento automatico per mezzo di reti neurali (ad esempio quella generativa), la computazione, comunicazione e sensoristica quantistica (di nuova generazione e non più prototipale) e la realtà estesa (con convergenza di realtà aumentata e virtuale), inducono una nuova visione e missione per i tradizionali ambiti d’applicazione della sicurezza cibernetica. Inoltre, gli impatti prospettici derivanti dall’adozione combinata di tali tecnologie saranno ancora più rilevanti in particolare sul quinto dominio, teatro di possibili conflitti militari in contesti geopolitici pronti, ma non sempre adeguatamente preparati, a fronteggiarsi in guerre ibride.

Si pensi, ad esempio, ad uno scenario futuro, tuttavia non così lontano dai giorni nostri, nel quale un agente di minaccia dalle ingenti risorse tecnico-economiche (ad es. uno stato nazione od un’organizzazione criminale internazionale) stesse, in modo non autorizzato, acquisendo ed archiviando da reti e sistemi dati cifrati dagli attuali ‘classici’ schemi crittografici (informazioni inintelligibili, alla data, poiché non interpretabili da chi non ne detenga le chiavi di decifratura).

Ipotizziamo, peraltro, che tale agente abbia poi accesso a tecnologie avanzate di intelligenza artificiale e computazione quantistica rese pubblicamente disponibili in una modalità a servizio sul cloud e possa, pertanto, avvalersi di algoritmi quantistici (ad esempio Shor per la fattorizzazione e Grover per ricerca) per decifrare dati precedentemente cifrati con algoritmi classici (potenzialmente vulnerabili con l’introduzione di elaboratori quantistici).

In tal contesto, l’attore di minaccia potrebbe avvalersi di modelli di apprendimento automatico quantistico (QML), per istruire la rete neurale con una notevole mole di informazioni riservate, segrete o, addirittura, militarmente classificate (precedentemente decifrate) e successivamente sfruttare l’intelligenza artificiale per individuare la catena d’attacco più efficace e impattante verso uno specifico bersaglio che si intendesse colpire ed al quale le informazioni apprese attenessero.

Le conseguenze di un attacco di tale portata sarebbero rilevanti poiché le capacità di prevenzione e contenimento degli impatti risulterebbero decisamente meno efficaci anche laddove si avvalessero delle medesime tecnologie della controparte. Questa ridotta efficacia delle contromisure deriverebbe dall’asimmetria nella ‘formazione’ delle intelligenze artificiali, quella offensiva e quella difensiva. Infatti l’intelligenza artificiale offensiva avrebbe accesso (non autorizzato) a dati di multiple organizzazioni mentre quella difensive non avrebbe modo di avvalersi della medesima quantità e qualità di dati (ma solo quelli della propria organizzazione) al fine di apprendere le migliori mitigazioni da attuare in quello specifico contesto, ovvero quello di un attacco mirato per il quale si è stati addestrati con informazioni di estremo valore.

Questo esempio proietta scenari di rischio ad alta complessità che inducono a riattualizzare le responsabilità associate al ruolo della sicurezza cibernetica. Un ruolo che merita di essere esteso in ampiezza e profondità, in modo duplice ed a mandati complementari:

- Un primo mandato è fortemente orientato ad avvalersi delle nuove tecnologie per due finalità distinte. La prima è quella di meglio fronteggiare le minacce emergenti, consci che gli agenti di minaccia ne gioveranno al contempo, ad esempio nelle tecniche di “deep fake” abilitate dall’intelligenza artificiale od in quelle volte allo “steal now, decrypt later” abilitate dalla computazione quantistica. La seconda finalità è invece volta ad agevolare ed arricchire l’esperienza digitale dell’individuo attraverso nuovi servizi innovativi che non prevedono solo di essere protetti dalla sicurezza ma la cui progettualità dovrebbe guidata dalla sicurezza digitale. Alcuni tipici esempi sono rappresentati dall’identità digitale nazionale ed europea, dal portafoglio digitale, dal voto elettronico, dai servizi fiduciari, dall’euro digitale, dai pagamenti su registri distribuiti, dalla federazione di fornitori di attributi personali, etc.
- Un secondo mandato è focalizzato ad indirizzare e proteggere nuovi prodotti e servizi digitali abilitati dalle nuove tecnologie, sulla base dei principi del ‘by design’, dal concepimento e la conseguente progettazione esecutiva, sino all’adozione in ambienti produttivi e su scala, attraverso le fasi implementative e di collaudo, in regimi tradizionali (waterfall) o agili (DevSecOps).

Alcuni esempi rappresentativi e significativi di nuovi ambiti di applicazione della sicurezza sono rappresentati da:

- l'apprendimento automatico responsabile per ottimizzazione delle reti neurali ed i controlli preventivi e proattivi sull'input (prompt) e reattivi sull'output (model response) generato dai sistemi di intelligenza artificiale;
- la critto-agilità, ovvero la capacità di adeguare nel tempo gli schemi di crittografia adottatati nelle organizzazioni a fronte delle capacità computazionali della nuova generazione di elaboratori quantistici in via di realizzazione (stanti gli algoritmi di cifratura attuali: tradizionali e quantum-safe);
- l'identificazione ed attuazione di contromisure dinamiche volte alla data-privacy per le informazioni processate dai visori della nuova realtà estesa che arricchisce di dati e metadati l'esperienza sensoriale fisica e la combina con quella virtuale. Informazioni spesso sensibili condivise dalle comunità di utilizzatori, talvolta inconsciamente e pertanto senza consenso informato;
- La protezione cibernetica di prodotto ('embedded' per i nuovi, 'wrapped' per quelli datati o obsoleti) nell'era dell'internet delle cose che oggi conta dispositivi sempre più interconnessi e sensori, attuatori e trasduttori fisici dei quali potrebbe essere preso il controllo. Dispositivi che scaleranno di ordini di grandezza rendendone complesso il monitoraggio e la protezione.

Nel settore della sicurezza cibernetica, il capitale umano rimane e rimarrà centrale, lo spettro di competenze dei nuovi esperti di sicurezza dovrà tuttavia ampliarsi per padroneggiare tali tecnologie, come nuovi strumenti della professione. Oltre alla competenza in materia cibernetica, si renderà sempre più necessaria la conoscenza dei settori di industria nella quale è applicata e, ovviamente, una forte familiarità con le tecnologie emergenti.

In un futuro non così lontano, probabilmente interfacce neurali impiantabili nel cervello degli individui e collegabili in banda larga alla rete potenzieranno le capacità cognitivo-professionali anche degli operatori di questo settore che potranno quindi interagire e operare simbioticamente con l'intelligenza artificiale diventando, al contempo, parte della potenziale superficie d'attacco esposta. Una nuova sfida per la sicurezza cibernetica del futuro è già all'orizzonte.

Multi-Factor Authentication: è davvero una panacea?

A cura di Enrico Morisi

La Multi-Factor Authentication (MFA) si innesta in uno dei domini più importanti dell'Information Security, quello dell'Identity and Access Management.

Il tema dell'autenticazione è fondamentale e rappresenta una delle criticità di livello più elevato.

Come è noto, i tre principali vettori d'ingresso sfruttati nella fase di Reconnaissance, il primo stage della Cyber Kill Chain di attacco, sono rappresentati dal social engineering, dallo sfruttamento delle vulnerabilità tecnologiche e dalla conoscenza delle credenziali per l'autenticazione sui sistemi target, ampiamente disponibili sui mercati del Deep e Dark Web.

Quindi è di fondamentale importanza dotarsi di un layer di difesa predittivo, basato su attività di Threat Intelligence, per la continua ricerca e identificazione delle effettive minacce esterne, al fine di delineare un quadro molto chiaro degli asset che occorra gestire.

È decisivo focalizzarsi sulle cosiddette "root cause".

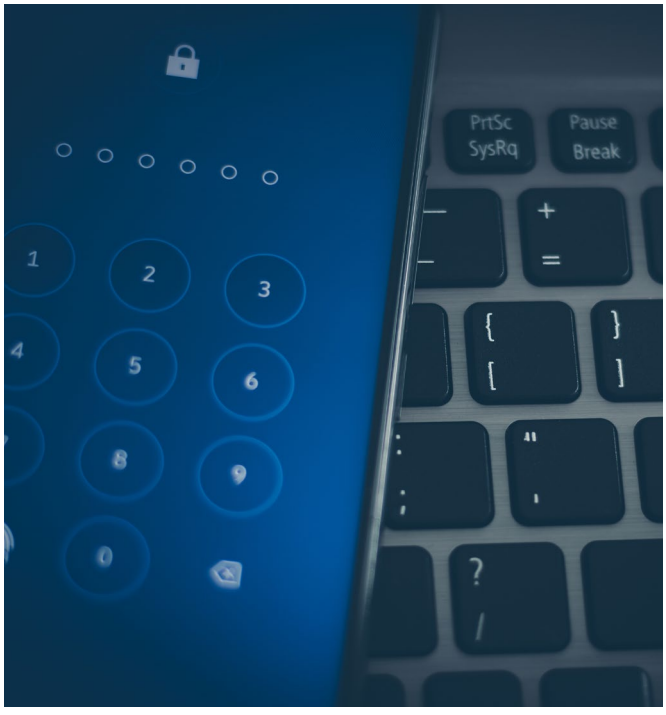
Preoccuparsi, ad esempio, del fenomeno "ransomware" senza chiedersi come possa essere somministrato all'interno di un'organizzazione, significa perdere di vista il vero rischio da valutare e mitigare.

Un'azione volta al contrasto di questi tre principali vettori d'ingresso comporta la mitigazione di molti rischi che un'organizzazione corre nell'ambito dell'Information Security, secondo alcuni addirittura fino al 90%, ed è fondamentale contemplarla nella definizione delle priorità, prestando ovviamente estrema attenzione anche a tutto il resto: sottovalutare un rischio, seppure "residuale", potrebbe costare molto caro perché non bisogna mai dimenticare che la cybersecurity è soprattutto una questione di dettagli.

Una delle strategie più efficaci ed economiche, e quindi più usate per il furto di credenziali, oltre alla diffusione di botnet, infostealer e RAT (Remote Access Trojan), e allo sfruttamento dei data breach, è lo stesso social engineering.

Social engineering e furto di credenziali rappresentano sostanzialmente due facce della stessa medaglia e sono utilizzati con successo in ben oltre la metà dei data breach andati a buon fine.

In un contesto di questo tipo, l'adozione di una soluzione basata su due o più fattori di autenticazione, che sia anche orientata a resistere ai più comuni attacchi di social engineering, costituisce un'azione di mitigazione imprescindibile ed estremamente efficace, rispondente alle logiche della strategia Zero Trust ed è talmente importante che non solo è annoverabile tra i primi progetti da gestire quando si decide di sviluppare un programma di Information Security per una data organizzazione, ma sarebbe da includere anche tra le metriche usate per mostrare al board i progressi raggiunti nel processo di mitigazione dei rischi emersi durante le attività di risk analysis.



I fattori di autenticazione si distinguono nelle seguenti tre tipologie che, se correttamente implementate, sono ritenute progressivamente più robuste, anche se non è da escludersi che pure le caratteristiche biometriche (le più "forti") possano essere compromesse e, quando lo sono, per loro natura lo sono per sempre (e.g. furto, spoofing, skimming e replay attack):

- qualcosa che si conosce, come password, PIN e passphrase;
- qualcosa che si possiede, in generale un dispositivo fisico come authenticator app, smartcard, token hardware e drive USB;
- qualcosa che si è, basato sul riconoscimento biometrico, come impronte digitali, scansioni facciali, della retina, dell'iride, del palmo della mano e della voce.

Esistono anche altri attributi che possono essere coinvolti e che fanno ricorso a forme adattive di autenticazione basate su policy context-aware che tengano conto ad esempio da dove, quando e con quale dispositivo avvenga l'autenticazione stessa.

Il fatto che una soluzione MFA sia "phishing resistant", semplicemente perché in grado di mitigare significativamente i più comuni attacchi di social engineering sferrati a danno della MFA stessa, come ad esempio il classico attacco Man-In-The-Middle, non significa però che sia "unphishable" o, più in generale, "unhackable".

In presenza di un end point compromesso, ad esempio, non esistono soluzioni MFA sufficientemente robuste, come anche nel caso di compromissione della "catena" di fornitura della soluzione stessa (e.g. caso "Twitter" dell'estate 2020).

Inoltre, le opzioni di "recover" previste in caso di malfunzionamenti, sono tipicamente meno sicure delle soluzioni MFA stesse, si pensi ad esempio al caso in cui sia previsto l'invio di un codice via SMS e a come questa funzione possa essere sfruttata da un attaccante che, spacciandosi per il fornitore del servizio coinvolto, la usi per una falsa richiesta di "verifica" del legittimo proprietario delle credenziali di accesso.

Un tema molto dibattuto e di grande attualità è poi quello sull'effettiva e reale robustezza del fattore di riconoscimento biometrico, in particolare negli scenari di autenticazione da remoto, tanto che ENISA ha recentemente pubblicato un report, delineando le best practice per il Remote IDentity Proofing (RIDP) alla luce della digital transformation che l'Unione Europea sta perseguendo (e.g. eIDAS 2.0 per un accesso sicuro e trasparente al EU Digital Identity Wallet) e che fa pesante affidamento sugli identificatori biometrici. Report che fornisce anche una panoramica piuttosto completa dei "biometric attack", identificando nel "deepfake presentation" e nel "data injection" le due minacce da mitigare più sfidanti.

Per non parlare del recente "game-changer", vale a dire l'individuazione di un malware in grado di rubare e potenzialmente usare gli attributi biometrici, non più solo password o codici generati dalla MFA (un trojan per iOS orientato, in particolare, al furto dei dati di riconoscimento facciale degli utenti, probabilmente prima che vengano memorizzati nel "Secure Enclave" chip o durante il loro uso).

Come raccomandato anche dal NIST nelle sue "Digital Identity Guidelines", anche gli attributi biometrici non dovrebbero essere usati come singolo fattore di autenticazione ma sempre abbinati ad un fattore fisico (e.g. FIDO2 security key).

Un'attenzione particolare andrebbe riservata alle soluzioni MFA, "phishing-resistant", sviluppate dalla Fast IDentity Online (FIDO) Alliance, in collaborazione con il World Wide Web Consortium (W3C) per la definizione di uno standard web che costituisce un componente chiave del set di specifiche FIDO2, basato sulla public key cryptography per la generazione di una coppia di cryptographic key (passkey) unica per ogni servizio, in abbinamento anche all'uso di attributi biometrici e orientato al tanto auspicato abbandono delle "famigerate" password, così complicate da gestire e così esposte al furto e agli attacchi di social engineering.

L'obiettivo non è mai il perseguimento della piena e completa sicurezza, che semplicemente non esiste, ma la mitigazione di un determinato rischio, considerato significativo per una data organizzazione.

Adottare una soluzione MFA che sia "phishing-resistant" va proprio nella direzione di ridurre la probabilità che possa essere compromessa, compensando il rischio residuale con, ad esempio, un'adeguata formazione, finalizzata a rendere consapevole l'utente finale di ciò che la soluzione adottata potrebbe non prevenire, educandolo a riconoscere e a disinnescare un eventuale attacco: potrebbe essere sorprendentemente efficace anche solo far presente di prestare attenzione a quando i successivi fattori di autenticazione vengono richiesti senza che sia stato innescato alcun voluto processo di autenticazione.

In definitiva, nonostante si tratti di una soluzione di fondamentale importanza e di evidente utilità, come ha scritto Bruce Schneier: "like all security technologies, MFA is not a panacea".

L’importanza strategica delle analisi di Threat Intelligence nella gestione della Supply Chain

A cura di Martina Fonzo

La globalizzazione e la digitalizzazione hanno trasformato la supply chain in un elemento fondamentale per le aziende moderne. Questa rete intricata di fornitori, partner e servizi è diventata il fulcro su cui si basa il successo e la competitività delle imprese. Tuttavia, con questa crescente interconnessione, sorgono anche rischi significativi che possono minacciare la sicurezza e la continuità operativa.

In passato, infatti, le sfide della supply chain erano principalmente legate alla logistica e alla produzione. Oggi, tuttavia, le minacce informatiche, le vulnerabilità nei sistemi di sicurezza e le frodi digitali sono diventate una seria preoccupazione per le aziende di ogni settore. Un attacco informatico o una violazione della sicurezza in uno dei partner della supply chain possono avere conseguenze devastanti sull’intera rete di approvvigionamento.

Immaginiamo una grande azienda di produzione che dipende da diversi fornitori per i componenti chiave del proprio prodotto. Se uno di questi fornitori subisce un attacco informatico e le sue credenziali vengono compromesse, gli attaccanti potrebbero ottenere accesso non autorizzato ai dati sensibili e alle informazioni proprietarie dell’azienda. Questo potrebbe portare non solo a una perdita di dati critici, ma anche ad una interruzione delle attività di produzione, ritardi nelle consegne e perdite finanziarie significative.

In aggiunta, con l’incremento della digitalizzazione dei processi aziendali, le transazioni finanziarie e le informazioni dei clienti sono sempre più spesso conservate e condivise online. Nel caso in cui un fornitore di servizi cloud incaricato della gestione dei dati finanziari aziendali subisca un attacco, le conseguenze possono essere catastrofiche: dati finanziari sensibili potrebbero essere esposti, mettendo a repentaglio la reputazione dell’azienda.

Consideriamo un’altra situazione: supponiamo che un fornitore di servizi logistici responsabile della distribuzione dei prodotti aziendali abbia il suo sistema di tracciamento delle spedizioni compromesso. In questa eventualità, l’azienda potrebbe trovarsi nell’impossibilità di monitorare accuratamente la logistica dei propri prodotti. Questa situazione potrebbe tradursi in ritardi nelle consegne, insoddisfazione da parte dei clienti e un calo della fiducia nel marchio.

In questo scenario, l’importanza delle analisi di Threat Intelligence diventa evidente per garantire la protezione e la sicurezza della supply chain digitale. Questo approccio si focalizza sull’osservazione e l’interpretazione dei dati relativi alle minacce informatiche, permettendo

alle aziende di identificare, valutare e mitigare i rischi in modo proattivo, fornendo una base solida per adottare le giuste contromisure.

I criminal hacker sono infatti sempre alla ricerca di punti vulnerabili all'interno della supply chain, e spesso trovano un bersaglio ideale nei fornitori di servizi. Questi fornitori gestiscono enormi quantità di dati sensibili e hanno accesso a sistemi che regolano l'intera catena di produzione e distribuzione. Inoltre, non è insolito che tali sistemi presentino falle di sicurezza, le quali, se sfruttate, possono compromettere l'intera catena di approvvigionamento.

Entrando nel pratico, immaginiamo un possibile scenario di attacco di phishing contro un fornitore di servizi cloud. Uno dei dipendenti riceve un'e-mail apparentemente legittima che lo invita a cliccare su un link per "aggiornare le credenziali di accesso al sistema". Ignaro del pericolo, l'impiegato inserisce le proprie credenziali, che vengono prontamente rubate dai criminal hacker. Una volta che gli attaccanti ottengono le credenziali del fornitore, possono facilmente accedere ai sistemi dell'azienda.

L'importanza delle analisi di Threat Intelligence diventa evidente per garantire la protezione e la sicurezza della supply chain digitale.

Una volta all'interno, individuano e sottraggono le credenziali di accesso interne memorizzate, se presenti. Questo significa che le informazioni sensibili non solo del fornitore ma anche dell'azienda finiscono nelle mani sbagliate: le informazioni personali di dipendenti e clienti, come nomi, indirizzi, e-mail e numeri di carte di credito, ma anche l'accesso ai sistemi di pagamento dell'azienda, provocando transazioni fraudolente o addirittura rubando direttamente fondi. Inoltre, rilevanti sono i rischi riguardo al furto di proprietà intellettuale, come segreti commerciali, brevetti e formule aziendali, tutte informazioni che possono danneggiare la posizione competitiva dell'azienda sul mercato.

Questo esempio sottolinea l'importanza cruciale dell'analisi di Threat Intelligence per garantire la continuità operativa delle aziende e proteggere i dati sensibili. Una solida Threat Intelligence avrebbe permesso di rilevare in anticipo le attività sospette nei sistemi del fornitore, prima che l'attacco si diffondesse ulteriormente. Questa prontezza nell'individuazione avrebbe dato alle aziende il tempo necessario per attuare le adeguate contromisure di sicurezza, proteggendo così i loro dati e le loro operazioni critiche. In questo modo, l'analisi non solo permette di reagire in modo efficace agli attacchi, ma anche di anticiparli, garantendo un livello superiore di sicurezza nella supply chain.

Inoltre, questo consente alle aziende di pianificare strategie di business continuity, garantendo operazioni ininterrotte anche in situazioni critiche. Essenziale è anche la condivisione delle informazioni di Threat Intelligence all'interno della supply chain. Questo scambio permette a tutti i partner di essere consapevoli dei rischi e di adottare misure preventive per proteggere l'intera catena di approvvigionamento.

Nel contesto di un mondo digitale sempre più interconnesso, la sicurezza della supply chain è diventata una priorità strategica per le aziende moderne. La Threat Intelligence fornisce le conoscenze e gli strumenti necessari per affrontare le minacce emergenti, proteggere l'integrità e la riservatezza dei dati e garantire la continuità operativa. Investire in pratiche avanzate di analisi e protezione delle minacce non è solo una necessità, ma un pilastro fondamentale per il successo e la sostenibilità a lungo termine delle aziende e della supply chain. Con una solida base di Threat Intelligence, le aziende possono essere pronte ad affrontare le sfide in continua evoluzione del panorama cyber, proteggendo così la propria reputazione e il proprio valore aziendale.

AI – Domande e riposte facili facili: l'AI per la scienza e la medicina

A cura di Gianpiero Cozzolino

Come si utilizza l'AI in ambito scientifico e medico?

Quando si utilizzano sistemi di apprendimento su immagini, si possono ottenere ottimi (cioè: superiori alle comuni capacità umane) risultati nel riconoscimento di elementi o schemi ricorrenti che possono poi, di conseguenza, essere utilizzati come sistemi di predizione rispetto ad alcuni aspetti.

Nello scorso Cyber Magazine, Petra Chiste, ci ha presentato la situazione dei GAP nel mondo delle discipline STEM (Science, Technology, Engineering, and Mathematics - Scienza, Tecnologia, Ingegneria e Matematica).

Per mia ignoranza mi sono andato a documentare, da qualche tempo si è compresa la necessità di unire le forze e le risorse verso un mondo dove tutti gli aspetti "scientifici" convergano per cercare nuove vie e soluzioni a problemi di una singola materia.

Un esempio banale: come faccio a fare una foto da 40 miliardi di pixel? È qui che entra in campo lo STEM, un approccio multidisciplinare per affrontare la sfida con molte più frecce nella faretra.

Quali sono i maggiori risultati nella medicina?

La medicina utilizza sempre di più sistemi diagnostici basati su dati oggettivi, siano essi in forma di immagine (reale, quando si usano telecamere, o virtuale, quando si usano sensori tipicamente a ultrasuoni o radiologici) che semplicemente numerica (come le analisi cliniche o i diagrammi temporali). Ciò corrisponde ad avere un'immensa base di dati su cui effettuare degli apprendimenti, dopodiché l'analisi di nuovi dati costituisce un ausilio per i medici, che possono concentrarsi sugli aspetti più complessi.

La base dati può anche non essere puramente medica: un altro aspetto interessantissimo è l'incrocio delle informazioni sanitarie con quelle delle abitudini dei pazienti (consumi, comportamenti, alimentazione), che possono quindi dare importanti risultati nella comprensione dei rischi rispetto alle patologie, anche con anni di anticipo, e mettiamoci anche un pizzico di DNA.

Il rovescio della medaglia è che queste basi di dati costituiscono un grandissimo rischio rispetto agli aspetti di privacy e di etica nei vari campi di ricerca. Ovviamente, un sistema automatico, per quanto possa essere di buona qualità, non può sostituirsi in toto ai medici ed ai comitati di controllo, né dal punto di vista pratico che da quello giuridico, fino a quando?

Quali sono gli utilizzi nella ricerca scientifica?

Moltissimi campi possono essere aiutati dai sistemi di apprendimento tipici dell'AI.

Nel campo farmaceutico, possono essere velocizzate la sintesi e la sperimentazione iniziale (cioè: prima di arrivare all'uomo) di nuove molecole farmaceutiche.

Similmente possono essere "pensati" nuovi materiali e sostanze per vari tipi di utilizzi.

In campo aerospaziale possono essere accelerate le analisi delle immagini dei telescopi, sia riguardo alla ricerca astrofisica che riguardo al monitoraggio di oggetti (artificiali o meno) vicini alla Terra; nonché per l'analisi dei segnali elettromagnetici di cui è investito il nostro

pianeta, potenzialmente portatori di contatti alieni.

Anche il monitoraggio ambientale può essere fortemente aiutato dall'analisi delle immagini della superficie terrestre, siano esse satellitari o meno (es. droni ed aerei).

Infine, pensando invece alle analisi di testi, alcuni algoritmi di AI potrebbero essere sviluppati per lo screening e pre-valutazione degli articoli scientifici, in modo da eliminare rapidamente quelli che hanno mancanze rispetto agli standard previsti.

Oggi si scansiona una pergamena sepolta dalla cenere vulcanica, dopo 2000 anni, senza toccarla analizzando le stratificazioni, le risposte differenti della pigmentazione, srotolandola digitalmente e facendo uso di OCR, su qualcosa che non si è neanche mai visto.

Che ne penso?

Qui è il vero campo di battaglia dell'AI, dove lo strumento consentirà di fare passi in avanti e costruire nuovi sensi oltre a quelli conosciuti, un "occhio" capace di vedere le distorsioni magnetiche, una "mano" capace di piegare gli atomi, un "orecchio" per sentire il tremito del tempo sull'orlo di un buco nero, tutti questi nuovi ed ignoti sensi verranno poi amalgamati in un insieme di dati e qui saremo sempre sull'oro del magico o della stregoneria, come nel medioevo dove i terrapiattisti se la ridevano di brutto.

Ma per ogni nuovo dato estratto e creato dovremmo avere un'etica umana, di come sfruttarlo ed usarlo; da una parte facendo un esame a 10 anni potremmo prevedere quando inizieremo a "stempiarci", dall'altro le lobby potranno modellare il gregge sulle scelte di vita...

Visione Negativa: "Non ti assicuro!! Sei un soggetto ad alto rischio";"ti faccio sentire un incapace, così posso pagarti meno!!"; "Mangia cavallette e formiche, così oltre a non inquinare, aiuti il GAP alimentare globale".

Visione Positiva: "immergiti in questo corso multi sensoriale che ti aiuterà ad evolvere il tuo senso critico"; "mangia questo formaggio almeno una volta per la vita"; "prendi questa pasticca dove all'interno ci sono le 163 dosi che ti aiuteranno a vivere in salute per almeno 250 anni"; "non c'è bisogno di rincorrere le lancette delle ore il tuo valore è nella tua capacità di relazione".

A noi accavallati a questo nuovo millennio il compito di indirizzare il futuro dell'umanità, se continuiamo a misurarci con il denaro le possibilità di vincere sono veramente scarse, e non mi metto neanche a commentare il motivo, c'è ora la possibilità di attuare nuovi valori: sociali, etici, climatici, scientifici.

Moltissimi campi possono essere aiutati dai sistemi di apprendimento tipici dell'AI.

L’Attribute Based Encryption per sfruttare al meglio i dati e ridurre il rischio di compromissione

A cura di Dolman Aradori

Il futuro della privacy dei dati è la fine della loro compromissione. Con il mondo che produce informazioni a ritmi sorprendenti, abbiamo bisogno di trovare un modo per utilizzare i dati al pieno della loro potenzialità proteggendoli allo stesso tempo dal rischio di una violazione e garantendo privacy, protezione e controllo dell’accesso.

Questi principi solo alla base dell’Attribute Based Encryption (ABE), una nuova forma di crittografia che, dopo anni di studio, comincia ad avere interessanti applicazioni anche a livello commerciale.

Tradizionalmente, la crittografia asimmetrica si basa su un sistema di chiavi pubbliche e private, dove la chiave pubblica viene utilizzata per cifrare i dati e la chiave privata per decifrarli. Più precisamente, solamente un’unica chiave può decifrare i dati criptati. In questo caso, chi detiene la chiave di decifratura accede a tutti i dati decriptati e chi non possiede tale chiave non ottiene, ovviamente, alcuna informazione.

D’altro canto, un individuo potrebbe voler condividere in modo selettivo i propri dati personali e documenti. Analogamente, un’azienda potrebbe voler condividere dati con diversi insiemi di utenti, in funzione delle loro credenziali. Idealmente, vorremmo poter criptare i dati in modo tale da garantire un controllo degli accessi puntuale e la capacità di eseguire calcoli in modo selettivo direttamente sui dati criptati.

Con l’ABE l’accesso ai dati cifrati non dipende solo dalla chiave privata, ma anche da una serie di attributi che devono essere soddisfatti.

Grazie all’ABE, infatti, è possibile associare attributi specifici ai dati sensibili e definire politiche di accesso basate su combinazioni di attributi. Questo apre la strada a una gestione più flessibile dell’accesso ai dati, consentendo di definire politiche di accesso personalizzate e raffinate in base a una vasta gamma di attributi come il ruolo dell’utente, la posizione geografica, l’orario di accesso e molti altri ancora.

Il paradigma quindi si sposta dal “tutto o niente” al “sia l’uno che l’altro”. Da una parte l’accesso a dati critici per chi sia in possesso dell’opportuna autorizzazione e contemporaneamente una solida cifratura dei rimanenti dati che devono invece continuare ad essere protetti.

Nella crittografia basata su attributi, i dati criptati sono associati ad attributi ed a chiavi di decifratura segrete, insieme a regole che stabiliscono quali dati cifrati possono essere decriptati da quali chiavi. Ad esempio, un fornitore di contenuti digitali può stabilire che nei giorni feriali una data chiave di decifratura permette l’accesso ai contenuti standard e premium e l’accesso a solo quelli standard nei giorni festivi. In applicazioni quali il data mining su dati medici cifrati o su dati provenienti da reti sociali, può essere utile fornire accesso parziale ai dati e permettere di eseguire elaborazioni sui dati criptati, come, ad esempio, permettere di calcolare statistiche o eseguire interrogazioni.

I casi d’uso di questo approccio basato sulle politiche sono convincenti e dietro di essi si trova un fondamento teorico distintivo.

La storia di ABE risale a un articolo innovativo del 2005 intitolato “Fuzzy Identity-Based Encryption”. Quindici anni dopo, riconoscendo l’importanza di tale documento, l’Associazione internazionale per la ricerca crittografica (IACR, International Association for Cryptologic Research) gli ha assegnato il premio Test of Time per il 2020.

L’eleganza di questo approccio è che protegge i dati attraverso la crittografia e, incorporando meccanismi di controllo dell’accesso direttamente nei dati, garantisce una protezione adeguata in ogni momento, indipenden-

temente dal sistema o dall'ambiente. Questo vantaggio unico migliora significativamente il tradizionale controllo degli accessi basato sul sistema.

L'Attribute Based Encryption offre soluzioni innovative per la gestione dell'accesso ai dati sensibili e trova applicazione in una vasta gamma di scenari come:

Il futuro della privacy dei dati è la fine della loro compromissione.

Distribuzione dei contenuti: l'ABE può essere impiegata per il controllo basato sul contenuto nell'accesso ai dati. Ad esempio, in ambito di distribuzione di contenuti digitali come video, musica o documenti, è possibile cifrare il contenuto utilizzando l'ABE e specificare politiche di accesso basate su attributi come l''età, il genere o la posizione geografica. Ciò consente di garantire che solo le persone con gli attributi appropriati possano accedere al contenuto.

Condivisione sicura dei dati: l'ABE può essere utilizzata per implementare politiche di accesso basate sui ruoli nelle condivisioni sicure dei dati. Ad esempio, in un ambiente aziendale, l'ABE può essere impiegata per consentire l''accesso ai dati sensibili solo ai dipendenti con un determinato ruolo aziendale, come i manager o i membri del team di ricerca e sviluppo. Ciò garantisce che solo le persone autorizzate possano accedere ai dati rilevanti per le loro responsabilità.

Protezione della Privacy: L'ABE può essere utilizzata per proteggere la privacy nella gestione dei portafogli elettronici. Ad esempio, in un sistema di pagamenti digitali, l'ABE può essere utilizzata per cifrare i dati del portafoglio e consentire l'accesso solo alle transazioni autorizzate dagli attributi corrispondenti. Ciò fornisce un livello aggiuntivo di sicurezza e privacy per gli utenti che desiderano proteggere le proprie informazioni finanziarie.

Implementazione di controlli antifrode nelle operazioni dispositive bancarie: l'ABE può essere utilizzata per autorizzare e proteggere le transazioni bancarie, contribuendo a contrastare le frodi. Ad esempio, in una transazione bancaria, l'ABE può essere impiegata per cifrare i dettagli dell'operazione utilizzando attributi come la posizione geografica, l'orario e l''importo. La banca può inviare un "challenge" cifrato all'utente, che dovrà dimostrare di possedere una chiave che può decifrare il challenge per ottenere l'autorizzazione. Ciò aggiunge un ulteriore livello di sicurezza e protezione contro le frodi.

Questi sono solo alcuni esempi di come l'ABE può essere applicata in diversi contesti. La flessibilità dell'ABE consente di adattarsi a molteplici scenari e di garantire un accesso sicuro e controllato ai dati sensibili.

L'ABE può essere integrata con altre tecnologie di sicurezza, come la crittografia omomorfica o la blockchain, per creare soluzioni ancora più robuste e sicure. L'interazione tra queste tecnologie può aprire nuove possibilità e applicazioni per l'ABE, consentendo una protezione avanzata dei dati sensibili in scenari complessi.

In conclusione, il velocissimo progresso delle tecnologie informatiche, delle reti di telecomunicazioni ad alta velocità e l'enorme proliferazione di dispositivi mobili ha avuto – e continua ad avere – un impatto molto profondo sulla nostra società. In particolare, negli ultimi anni, abbiamo assistito ad uno spostamento progressivo ed inesorabile delle capacità di calcolo e di archiviazione dati nel cloud. Senza adeguate contromisure, rischiamo devastanti falle nella nostra privacy o, ancor peggio, rischiamo di vivere in uno stato di perenne sorveglianza digitale.

L'Attribute Based Encryption rappresenta un importante passo avanti nella protezione dei dati sensibili e nel controllo degli accessi. Il suo futuro è promettente, con miglioramenti nell'ambito delle prestazioni, dell'interoperabilità, dell'integrazione con altre tecnologie senza trascurare la resistenza quantistica. Continuerà ad evolversi per soddisfare le crescenti esigenze di sicurezza dei dati e fornire soluzioni innovative per una vasta gamma di scenari applicativi.

I nuovi Trend dello scenario cybercriminale

A cura di Sofia Scozzari

Negli ultimi 13 anni, l'analisi dei cyber attacchi che abbiamo svolto ci ha consentito di comprendere il variegato e movimentato panorama delle minacce digitali.

Analizzando e classificando le informazioni provenienti da attacchi di successo e di pubblico dominio, abbiamo potuto individuare le falle nelle misure difensive e le azioni di mitigazione necessarie, facilitando lo sviluppo di strategie di Cyber Security più efficaci in uno scenario cyber criminale in continua evoluzione.

Ogni anno, infatti, abbiamo visto crescere sia il numero di cyber attacchi che i relativi impatti per le vittime.

Anche il 2023 ha mantenuto le premesse, regalandoci però qualche sorpresa extra.

Lo scenario globale

In totale, a partire dal 2011, abbiamo classificato oltre 23.000 cyber attacchi.

Di questi, il 71% è avvenuto negli ultimi 6 anni indicando una chiara accelerazione nelle attività cyber criminali.

Nel 2023 per la prima volta abbiamo incluso nelle nostre analisi anche informazioni collezionate dal Dark Web evidenziando un'escalation notevole nella frequenza e nella complessità degli incidenti, con un incremento del 184% rispetto all'anno precedente e un totale di 7.068 cyber attacchi a livello globale, contro i 2.489 dell'anno precedente.

Anche le medie mensili hanno mostrato lo stesso andamento, passando da 207 attacchi in media al mese nel 2022 a 589 nel 2023. Di questi, 406 sono gli attacchi che abbiamo rilevato mediamente ogni mese nel Dark Web.

Storicamente l'andamento mensile delle attività cyber criminali mostra un calo all'inizio e alla fine dell'anno e un picco in primavera. Nel 2023 questo picco si è verificato ad aprile con 763 attacchi, mentre a gennaio e febbraio si è registrato il minor numero di incidenti.

Il peso del Dark Web

Con il termine "Dark Web" si intende la parte di Internet nascosta, non indicizzata dai motori di ricerca convenzionali ed accessibile solo tramite software specifici, come ad esempio Tor (The Onion Router), in grado di nascondere l'identità degli utenti.

Il Dark Web è comunemente noto per ospitare attività illecite, come il commercio di droghe e armi, ma anche di dati rubati e software malevoli.

Alcuni degli incidenti che abbiamo analizzato e classificato a partire dal monitoraggio delle fonti sul Dark Web, sono stati successivamente rilevati anche nel web tradizionale.

Abbiamo però constatato che nel 2023 questa porzione ammonta solo al 39%, mentre oltre due terzi degli attacchi è rimasto esclusivamente notificato nel Dark Web, evidenziando quindi che molte minacce significative non vengono rilevate nei canali convenzionali.

L'analisi delle fonti nel Dark Web ha quindi enfatizzato un fenomeno più vasto di quanto avevamo preventivato e la necessità di continuare a monitorare ed estendere i canali di ricerca, oltre a quelli tradizionali.

Ignorare le attività malevole che avvengono nel Dark Web potrebbe comportare notevoli rischi per le aziende, tra i quali l'esposizione a violazioni e compromissioni di dati venduti o messi a disposizione illegalmente a seguito di attacchi o data breach (anche di terze parti!), danni alla reputazione, perdite finanziarie, ecc.

Le motivazioni degli attacchi

Il predominio del cybercrime come motivazione principale degli attacchi è ormai una costante da anni.

Nel 2023 le attività cybercriminali ammontano al 93% del totale, addirittura in crescita rispetto all'anno precedente (82%).

Il continuo incremento di questo ambito mette in evidenza un trend allarmante delle attività cyber criminali organizzate e sofisticate, suggerendo che gli attaccanti stanno diventando sempre più audaci e innovativi.

Per quanto riguarda le altre categorie, le attività imputabili a Espionage / Sabotage e Information Warfare decrescono rispetto al 2022.

In leggera crescita, invece, il fenomeno dell'Hacktivism (dal 3% al 4%), ma, come abbiamo potuto constatare, i danni associati a questa tipologia di attaccanti sono di norma inferiori rispetto alle precedenti.

Tra i gruppi cyber criminali più attivi, LockBit 3.0 ha il primato assoluto con 1.041 cyber attacchi censiti nel 2023, seguito da ALPHV/BlackCat (417), Play (311), 8Base (279) e BlackBasta (187).

La distribuzione delle vittime

Nel 2023 i settori maggiormente impattati dai cyber attacchi sono Manufacturing (16% degli incidenti classificati), Professional / Scientific / Technical (11%), ICT (10%), Healthcare (9%) e Financial / Insurance (8%).

La principale differenza rispetto all'anno precedente riguarda la categoria "Multiple Targets", ovvero gli obiettivi multipli, che nel 2022 rappresentava la vittima principale (22% degli attacchi) mentre nel 2023 viene impattata solo dall'8% degli incidenti, a riprova del fatto che le attività malevole cyber criminali stiano diventando più mirate verso bersagli precisi.

Ne è la prova anche la geografia delle vittime che mostra una crescente predilezione per le azioni cybercriminali mirate e meno dispersive. Nel 2023, infatti, diminuiscono considerevolmente gli attacchi verso bersagli situati in località multiple, passando dal 29% nel 2022 al 9%.

Tornano invece a crescere le vittime in America, che si attesa al 50% degli incidenti, dopo la flessione degli anni precedenti (era il 37% nel 2022), e in Europa, che, in costante aumento fin dal 2019, raggiunge la quota record del 27% degli attacchi (dal 24% dell'anno precedente), a riprova del fatto che il vecchio continente rappresenti ormai un obiettivo di sicuro interesse per i cyber criminali, impattato per quasi un terzo delle loro attività malevole.

In aumento anche gli attacchi verso Asia (dall'8% al 10%) e Africa (2% nel 2023), mentre restano sostanzialmente invariate le quote dell'Oceania (2%).

L'evoluzione delle minacce

Già dal 2018 il Malware è la tecnica di attacco più utilizzata dai cyber criminali.

Ma nel 2023 il ricorso a questa tecnica aumenta pericolosamente, arrivando quasi a raddoppiare e toccando il 70% del totale degli attacchi (rispetto al 37% del 2022), indice che i cyber criminali fanno sempre più affidamento sull'impiego di codice malevolo.

Seguono lo sfruttamento delle vulnerabilità (11%), in

leggero calo rispetto all'anno precedente, e le tecniche sconosciute (9%), in netta diminuzione rispetto al 24% del 2022, un ulteriore segnale che gli attaccanti prediligono a questo punto tecniche più affidabili e consolidate.

Sebbene raddoppiati in termini numerici, gli attacchi che fanno affidamento su Phishing e Social Engineering mostrano una flessione in termini percentuali (dal 12% al 3%), pur restando un consolidato veicolo di infezione e di distribuzione di malware.

Si riduce, inoltre, il ricorso a DDoS (dal 4% al 3%), tecniche multiple (dal 7% al 2%) e Identity Theft / Account Cracking (dal 3% all'1%).

I Web attack, che già negli anni precedenti rappresentavano una minima parte degli attacchi totali, continuano la loro decrescita e raggiungono a questo punto quota zero.

L'evoluzione significativa nell'uso di malware, indica che gli attaccanti stanno perfezionando i loro strumenti e metodi per aggirare le difese esistenti, in particolare per quanto riguarda i ransomware che rappresentano la tipologia prediletta di codici malevoli (95% dei malware classificati).

Tra le famiglie di ransomware più utilizzate nel 2023, LockBit, ALPHV/BlackCat, Play, 8Base, BlackBasta e Malas coprono rispettivamente le prime sei posizioni, rappresentando quasi la metà (49%) dei malware totali.

Gli impatti crescenti

Da anni abbiamo introdotto nella nostra analisi anche la valutazione degli impatti dei cyber attacchi, per monitorare, oltre all'incremento nel numero degli incidenti, i danni subiti dalle vittime, sia in termini economici, che tecnologici, operativi o reputazionali.

Nel 2023 gli attacchi con impatti gravi o gravissimi toccano un'impressionante quota del 91%, la più alta registrata finora, contro l'80% del 2022, mentre quasi un quarto degli attacchi (24%) ha avuto impatti critici.

Il netto incremento nelle severity dei cyber attacchi sottolinea la crescente capacità degli attaccanti di infliggere danni significativi alle proprie vittime, con conseguenze sempre più serie e profonde implicazioni per la stabilità finanziaria, la sicurezza e la reputazione delle aziende.

Conclusioni

L'analisi dei trend evidenzia uno scenario cyber in continua evoluzione, caratterizzato da cybercriminali che si adattano e affinano le loro strategie per infliggere il maggior danno possibile alle vittime.

Riconoscere questa evoluzione ed implementare misure di sicurezza adeguate, sia preventive che reattive, è a questo punto un imperativo per le organizzazioni di ogni settore per consentire di mettere in atto una strategia difensiva in grado di fronteggiare questo panorama di minacce sempre più complesso.

CYBER
Think Tank
ASSINTEL

Disclaimer

Gentile lettore,

Ti informiamo che il contenuto pubblicato su questo magazine è fornito a scopo puramente informativo e di intrattenimento. Tutte le opinioni, idee e punti di vista espressi negli articoli sono esclusivamente quelli degli autori e non riflettono necessariamente l'opinione di Assintel o dei suoi redattori.

Tutte le informazioni fornite sono basate sulle conoscenze e le fonti disponibili al momento della pubblicazione. Tuttavia, non possiamo garantire l'accuratezza, l'integralità o l'aggiornamento delle informazioni fornite. Pertanto, l'utilizzo delle informazioni presenti su questo magazine avviene a proprio rischio e discrezione.

Si prega di tenere presente che il contenuto potrebbe evolvere nel tempo e potrebbe non essere più aggiornato o rilevante al momento della lettura. Pertanto, consigliamo di verificare sempre l'attualità delle informazioni fornite e di consultare professionisti qualificati per eventuali questioni specifiche o decisioni importanti.

Inoltre, il Cyber Think Tank di Assintel declina ogni responsabilità per eventuali errori, omissioni o danni derivanti dall'uso delle informazioni contenute nel presente magazine. Non siamo responsabili per qualsiasi rivendicazione, perdita o danno di qualsiasi tipo che possa sorgere direttamente o indirettamente dall'utilizzo delle informazioni qui presentate.

Ti invitiamo a fare affidamento su più fonti di informazione per ottenere una visione più completa e a considerare che i punti di vista espressi possono variare in base all'esperienza e alle opinioni personali degli autori.

Infine, vorremmo sottolineare che il magazine non fornisce consulenza legale, finanziaria, medica o professionale di alcun genere. Si consiglia di consultare sempre un professionista qualificato per risolvere eventuali questioni specifiche che riguardano la tua situazione personale.

Cordialmente

La redazione

CYBER
Think Tank
ASSINTEL

CYBER MAGAZINE

CYBER
Think Tank
ASSINTEL

Contattaci:

segreteria@assintel.it
www.assintel.it

ASSINTEL
ASSOCIAZIONE NAZIONALE
IMPRESE ICT