CYBER MAGAZINE

CYBER Think Tank ASSINTEL

Giugno - Luglio 2023

Cyber Think Tank Assintel

CYBER THINK TANK ASSINTEL

CHI SIAMO?

Il Cyber Think Tank Assintel, affianca le aziende utilizzando standard, best practice e le migliori tecnologie disponibili in commercio.

I NOSTRI VALORI

Il Cyber Think Tank Assintel è un hub di collaborazione in cui aziende e professionisti lavorano insieme per affrontare le sfide più pressanti in materia di sicurezza informatica.

Se non sei socio, associati e unisciti a noi nel prossimo meeting!

Prossimo incontro

18 luglio

Ore 14:30

Per info scrivi a:

segreteria@assintel.it

COORDINATORE:

Pierguido Iezzi

COMITATO SCIENTIFICO:

Antonio Assandri, Gianpiero Cozzolino, Vittorio Orefice

REDAZIONE:

Federico Giberti, Melissa Keysomi, Daniela Grossi, Elisa Buonocore

INDICE

CYBER THINK TANK ASSINTEL

WEBINAR BLOCKCHAIN

24 luglio

12:00- 13:00

RELATORI:

Pietro Azzara

Angela Carpano

Lorenzo Sala

Esplora le opportunità infinite nel nostro Webinar:
Connetti, Apprendi, Cresci!

Per info scrivi a:

segreteria@assintel.it

INDICE

L'editoriale del Coordinatore di Cyber Think Tank Assintel Pierguido Iezzi

Luglio 2023

Gentili lettori,

Siamo lieti di darvi il benvenuto al nuovo numero del Cyber Magazine del Cyber Think Tank di Assintel. In questa edizione, abbiamo selezionato una vasta gamma di articoli che affrontano argomenti di grande rilevanza nel campo della cyber security e della tecnologia digitale. Attraverso queste pagine, vi condurremo in un viaggio informativo che vi consentirà di approfondire la complessità e l'importanza di temi come la blockchain, la sicurezza informatica, l'analisi delle tecniche di social engineering, la protezione dei dati, la governance dell'IA e molto altro ancora. Siamo entusiasti di condividere con voi questa variegata selezione di articoli che ben rappresentano la complessità e la rilevanza del panorama cyber attuale. Speriamo che questo secondo numero del Cyber Magazine vi offra nuove prospettive e vi stimoli a continuare a esplorare il sempre più complesso panorama della sicurezza informatica e dell'innovazione tecnologica.

Buona lettura!

Pierguido Iezzi

Threat Sharing: l'unione fa la forza

A cura di Pierguido Iezzi

Imparare dalle esperienze altrui – in particolare nel mondo della cyber security – è un concetto da molti abbracciato, ma che trova risicate corrispondenze nel quotidiano.

D'altronde, i Criminal Hacker hanno dalla loro parte il vantaggio di sperimentare e testare nuovi exploit quotidianamente, mentre i CISO, CIO e Security Expert si vedono costretti ad una partita "in rincorsa".

Dai forum ai market sul Dark web, tra gli aggressori vige una certa libertà di circolazione delle informazioni, in particolare quando si tratta di nuove vulnerabilità. Tra aziende, questo tipo di sinergia è fisiologicamente più difficile da impostare.

Ecco dove entra in gioco il Threat Infosharing, la forma più "pura" di condivisione delle informazioni sulle minacce a vantaggio della resilienza del perimetro aziendale. Il Threat Infosharing si basa sulla condivisione reciproca di informazioni relative a minacce, vulnerabilità e attacchi tra organizzazioni, enti governativi, provider di servizi e altri soggetti coinvolti nella sicurezza informatica. Questa pratica consente di creare una rete di collaborazione e scambio di conoscenze che permette di rilevare e rispondere alle minacce più rapidamente ed efficientemente di quanto sarebbe possibile se ogni entità operasse in modo isolato. È il mantra del ***"scientia potentia est"*** di Bacon applicato alla sicurezza informatica. Il Threat Infosharing aiuta ad ampliare percezione e awareness per tutte le organizzazioni coinvolte, a tutti i livelli. Questa condivisione proattiva delle informazioni sugli attacchi crea una catena difensiva tra le organizzazioni che partecipano alla comunità, sviluppando un'immunità di gregge contro attacchi che altri hanno riscontrato nelle proprie reti.

Il Threat infosharing, la forma più "pura" di condivisione delle informazioni sulle minacce a vantaggio della resilienza del perimetro aziendale.

Una questione di fiducia

Naturalmente, ci sono preoccupazioni riguardo alla condivisione di informazioni con chiunque. La condivisione richiede fiducia. Le imprese sono più propense a condividere informazioni informalmente, dietro porte chiuse, con partner e attraverso discussioni personali. Questo è da sempre lo scoglio culturale più difficile da superare, ma l'esperienza dimostra come senza collaborazione, i tempi di risposta si allungano, le aziende sono generalmente impreparate e non c'è coordinazione tra aziende o settori quando si scopre una minaccia di livello critico, pensiamo al caso Kaseya del 2021.

Proprio la rapidità è uno dei punti forti del Threat Infosharing, è forse uno dei pochi strumenti in grado di mantenere la stessa velocità con cui le minacce informatiche si evolvono. Quando una particolare minaccia viene individuata da un'organizzazione, la sua condivisione con gli altri membri della comunità del Threat Infosharing permette di avvisare rapidamente le potenziali vittime e di adottare contromisure appropriate per mitigare l'impatto.

Inoltre, il Threat Infosharing consente di raccogliere dati e informazioni da una vasta gamma di fonti. Questo offre una prospettiva più ampia sul panorama delle minacce e permette di identificare correlazioni e modelli che potrebbero non essere visibili da singoli attori isolati. Attraverso l'analisi dei dati condivisi, è possibile individuare indicatori di compromissione (IOC) comuni, riconoscere le caratteristiche distintive degli attacchi e comprendere meglio i modi in cui gli aggressori operano. Questa conoscenza condivisa può essere utilizzata per sviluppare e migliorare le difese e le strategie di mitigazione delle minacce. Un altro beneficio del Threat Infosharing è la possibilità di imparare dagli altri. Le organizzazioni che partecipano a tali comunità di condivisione delle informazioni possono acquisire conoscenze e competenze da esperti in sicurezza informatica, da enti governativi e da altre realtà che hanno già affrontato situazioni simili. Questa collaborazione favorisce l'innovazione e la diffusione di best practice. Tuttavia, è importante sottolineare che questo mondo deve essere gestito con cura per garantire la riservatezza delle informazioni sensibili e dei dati personali. I partecipanti devono adottare protocolli e framework adeguati per proteggere le informazioni condivise e rispettare le normative sulla privacy vigenti.

Lavorare insieme e imparare dagli altri aiuta a costruire una comunità resiliente e preparata ad affrontare le sfide del mondo digitale in continua evoluzione, questo è anche il mantra del Cyber Think Tank Assintel che – per questo motivo – ha rilasciato la prima versione della sua piattaforma di Infosharing.

Sicurezza proattiva: quello che ho imparato negli ultimi 27 anni

(a.k.a. «Pentesting field experiences: 1996-2023»)

A cura di Raoul Chiesa

1. Introduzione: Il mio primo PT

Il mio primo Penetration Test (di seguito, “pentest”) lo eseguii nel 1996, l’anno successivo alla famosa “Operazione Ice Trap” che mi vide coinvolto, eseguita dalla SCO (Sezione Centrale Operativa) della Polizia di Stato, che si concluse il 13 dicembre del 1995. Dopo tre mesi e mezzo di domiciliari decisi - anche grazie alla comprensione, all’empatia ed al rapporto personale che si venne a creare con il PM del caso, il Dott. Saviotti della Procura di Roma, e la D.ssa Maria Cristina Ascenzi della SCO – di impiegare le mie capacità di Ethical Hacking professionalmente.

Decisi quindi di avviare la mia prima ditta individuale, la “Security First”, fornendo le prime consulenze tecniche e tecnologia basica (hardware e modem). In seguito fui ingaggiato da un amico di Torino, il quale gestiva un ISP, per effettuare una “simulazione d’attacco” nei confronti di un suo cliente, nella fattispecie un’azienda metalmeccanica di medie dimensioni.

A quel tempo, ovviamente, non c’era “Internet”, o quantomeno come la intendiamo nei giorni d’oggi: per capirci, VOL (VideoOnLine), il primo ISP italiano massivo, vide la luce nel 1994 grazie all’intuito di Nicola Grauso in quel della Sardegna (Nicola poi fondò Tiscali molti anni dopo). A quei tempi, le aziende che necessitavano di connettività distribuita, utilizzavano le Reti a Commutazione di Pacchetto (in Italia tale servizio veniva offerto da ITAPAC).

Ogni paese era dotato di una sua rete nazionale basata su protocollo X25, una sorta di enorme rete WAN distribuita ed altamente efficace.

Parliamo ovviamente degli albori delle telecomunicazioni informatiche e di una tecnologia concepita negli anni ’70 e sviluppatasi globalmente nel corso degli anni ’80.

Tornando al mio primo pentest, il target era un VAX/VMS della DEC (Digital Equipment Corporation): l’amico che mi ingaggiò sapeva che ero molto bravo sui VAX, ma quello che non sapeva era che li avevo sempre utilizzati e “testati” da remoto, X25 per l’appunto. In pratica, non avevo mai visto dal vivo un VAX/VMS, e non ero mai stato in “consolle”.

Purtroppo, quell’azienda metalmeccanica non aveva connessioni remote X.25, era presente solo un modem a 1200 Baud, davvero troppo lento per lanciare attacchi brute-force, ma, soprattutto, a causa della distanza logistica del cliente da Torino, la linea telefonica risultava essere estremamente disturbata ed instabile per poter lavorare da remoto via modem.

A questo punto per ovviare a tali criticità, decidemmo di recarci direttamente in azienda. Mai dimenticherò le sensazioni che provai vedendo e toccando un vero VAX quella prima volta. Imparai così ad operare “in locale” apprezzando ancor di più quel fantastico OS che era il VMS.

Il resto è storia… una storia vissuta in prima persona, attraverso le varie aziende che ho fondato o co-fondato, specializzandomi sempre di più, per quasi 30 anni, proprio nel Pentesting. Ma, come dico sempre, dobbiamo imparare dalla storia… e dalle mie storie di Pentest ho appreso davvero molto sul “mercato” della Proactive Security.

2. Introduzione: evoluzioni e status attuale

Da quel lontano 1996 ad oggi sono accaduti innumerevoli cambiamenti: la DEC fu acquisita dalla Compaq (la quale, a sua volta, fu acquisita da HP), le Sun Solaris e gli IBM Aix continuavano a venire venduti in tutto il mondo, le reti X.25 vennero mano a mano dismesse e l'IPv6 avrebbero reso divertenti le nostre vite da penetration tester, insieme al 5G e all'IoT/IoX.

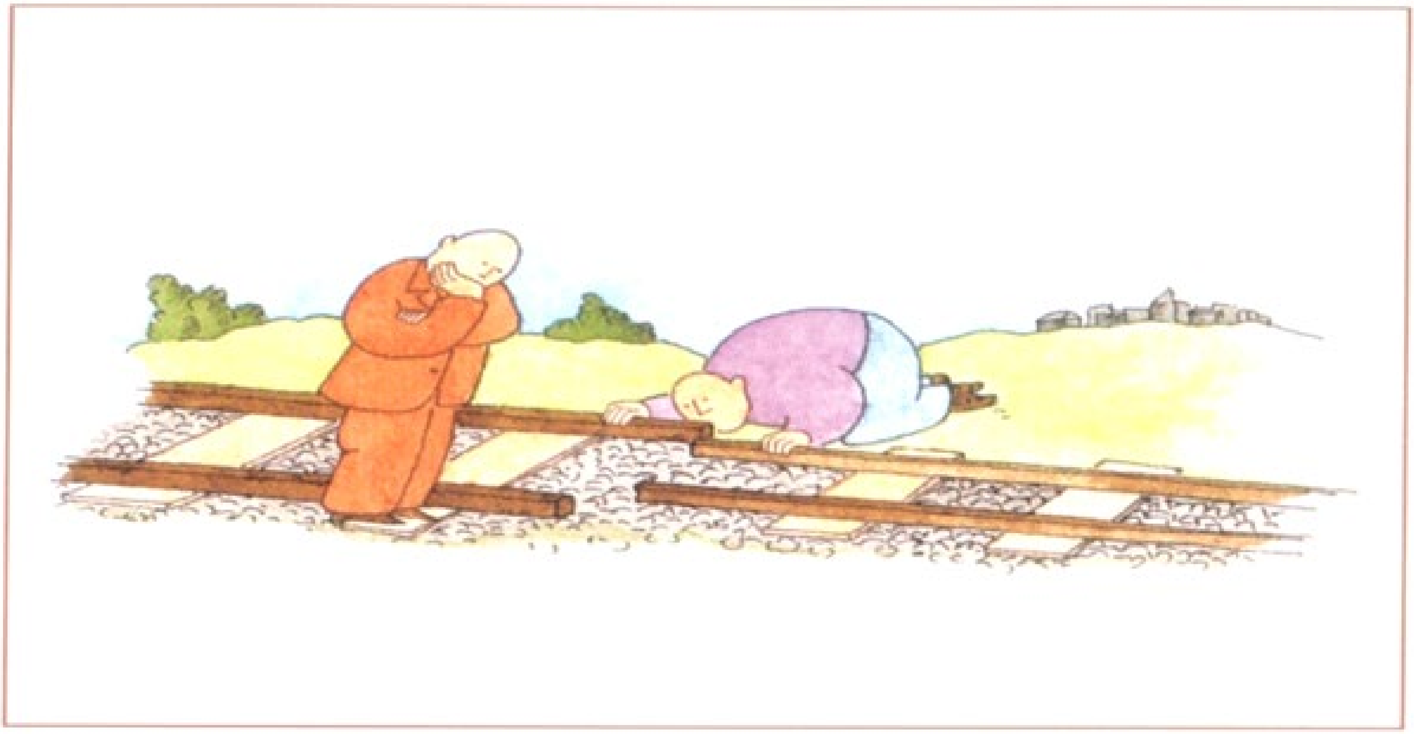
Nel 2000 entrai nel team di ISECOM (Institute for Security and Open Methodologies, USA), la community no-profit che ha regalato al mondo il fantastico OSSTMM (Open Source Security Testing Methodology Manual), permettendo di integrare una reale professionalità – ed una metodologia libera, gratuita e condivisa a livello mondiale, dal mondo militare e governativo sino alla Pubblica Amministrazione ed alle aziende private – al settore della Sicurezza Preventiva ("Proactive Security"), insieme a più di 10.000 volontari e dozzine di Key Contributors, tra i quali il sottoscritto.

Nonostante ciò, le organizzazioni e le aziende continuano a commettere diversi errori quando hanno a che fare con l'argomento del Penetration Testing: questo sia dal punto di vista strategico, che di business e delle prospettive operative.

L'obiettivo, con questa serie di articoli, è condividere le mie esperienze sul campo. Ritengo possa essere utile sia agli "op geeks" che ai manager evidenziare le procedure errate commesse da alcuni clienti (che hanno reso il nostro lavoro estremamente difficoltoso e dispendioso in termini di risorse umane e ore lavorative).

3. Problematica Uno: "Mindset" e background

Durante i training, nei corsi specializzati, e nei Master universitari dove insegno, ricorro frequentemente a questa rappresentazione grafica per descrivere il concetto di "Mindset".



L'esempio tipico che faccio è quello del dialogo tra un Auditor e un Pentester.

Nonostante operino entrambi nello stesso "settore" di nicchia (la "verifica" della sicurezza, possiamo dire per sintetizzare), utilizzano linguaggi e termini diversi, oppure gli danno significati differenti. Hanno difficoltà a comprendersi reciprocamente,avendo formazione ed esperienze diverse.

Ampliando questo concetto possiamo capire come il mindset ed il background (di studi e lavorativo) del committente possa creare sin dall'inizio una serie di problemi, quando si viene ingaggiati per un progetto di Penetration Test.

Infatti, a seconda della nazione e del continente, il "referente tecnico" dell'azienda cliente avrà almeno uno di questi profili:

- Tecnico IT esperto (ma NON un "InfoSec" guy)
- Tecnico IT con poca esperienza (teorica, ma soprattutto pratica)
- Infosec Guy inesperto (ma che magari si è "venduto bene")
- Auditor
- Risk Officer
- Privacy Officer / Legal
- Manager non tecnico
- Ex Forze dell'Ordine
- Infosec Guy realmente esperto (rari come il tartufo bianco ed i cigni neri!)

Le conseguenze, sin dalle fasi iniziali (prevendita, accordi tecnici, Target of Evaluation, Regole di Ingaggio, etc) possono essere "disastrose", o comunque non rendere facile il lavoro per il quale siamo stati ingaggiati:

- ► La maggior parte degli interlocutori – circa l'80% - non vi comprenderà a causa del differente linguaggio (il concetto appunto di Mindset e Background): slang tecnico, terminologie, acronimi, concetti di cybersecurity, metodologie e così via.
- ► Quasi tutti – circa il 95% - non ne saprà abbastanza sui penetration test, ma vorrà dire la sua.

Per concludere, nella "testa del cliente" troveremo sempre una o più di queste domande, talvolta addirittura anche a livello inconscio:

- Ho (davvero) bisogno di un test di sicurezza?
- Quanto spesso devo farlo?
- Chi dovrebbe eseguirlo?
- È meglio ingaggiare un consulente, un'azienda specializzata, o formare/utilizzare personale interno?
- Come scelgo il giusto fornitore?
- ... e comunque devo spendere il meno possibile!

Governare l’AI (OPEN ED)

Il caso ChatGPT: il diritto di non scegliere tra innovazione e libertà

A cura di Guido Scorza

Qualche mese fa, il Garante per la protezione dei dati personali italiani, primo al mondo, ha ordinato a OpenAI, la società che ha sviluppato e gestisce ChatGPT – sin qui la più famosa intelligenza artificiale generativa di tutti i tempi – di sospendere il trattamento dei dati personali raccolti in Italia o, comunque, relativi a persone residenti in Italia in ragione diverse, probabili violazioni della disciplina sulla privacy.

All’indomani, come è noto ai più, Open AI ha reso il proprio servizio inaccessibile dal nostro Paese.

Apriti cielo.

I social – e, per la verità anche alcune testate giornalistiche blasonate – sono letteralmente impazziti: l’Italia sembrava aver identificato in ChatGPT il « campione », in odor di santità, dell’innovazione e nel Garante per la privacy l’antagonista pagano, determinato a minacciare la « santa innovazione », a stelle e strisce.

Ne è nata un’autentica crociata nell’ambito della quale al grido « innovare, innovare, innovare », centinaia di migliaia di persone di estrazione diversissima hanno cominciato ad argomentare che la tutela del diritto alla privacy non avrebbe dovuto spingersi a bloccare l’innovazione e a dare, del nostro Paese, l’immagine di un Paese retrogrado e luddista.

Ma tutto questo, ormai, è storia o, almeno, dovrebbe esserlo.

Decine di Autorità in giro per il mondo, infatti, hanno cominciato a interrogarsi sulla legittimità di ChatGPT; a Bruxelles, in seno al Board dei garanti per la protezione dei dati personali (EDPB), è stata istituita una task force per identificare un approccio comune su una questione universalmente riconosciuta di straordinaria rilevanza e Sam Altman, il CEO di OpenAI, si è presentato davanti al Congresso americano chiedendo regole e vigilanza.

Insomma, nessun “caso Italia”, nessuna crociata italiana contro la santa innovazione.

Si era semplicemente identificato, magari con qualche settimana di anticipo, una questione che era e resta globale.

E, d’altra parte, oggi ChatGPT è di nuovo accessibile anche in Italia dopo che OpenAI ha adempiuto a un nuovo provvedimento, questa volta prescrittivo del Garante, rendendo il proprio servizio un po’ più trasparente e un po’ più rispettoso dei diritti e delle libertà delle persone.

Ma siamo solo all’inizio di una vicenda che è lontana dal potersi considerare conclusa – l’istruttoria è ancora alle sue battute iniziali – e che, comunque, è solo la punta dell’iceberg dei rapporti tra innovazione, regole, diritti e libertà ai tempi degli algoritmi e dell’intelligenza artificiale.

E quella di ChatGPT resta un’occasione utile per affrontare il problema – quello di metodo più che quello di merito – del governo del progresso tecnologico.

Vale, quindi, la pena, forse, mettere in fila alcune lezioni che la vicenda ci ha già consegnato.

Le regole servono a garantire diritti e libertà e garantirne l’applicazione – come ha fatto il Garante italiano con la sua iniziativa nei confronti di OpenAI - risponde alla stessa esigenza, un’esigenza irrinunciabile in democrazia e un’esigenza che non può, per definizione, mai porsi in antitesi con l’innovazione, almeno se si crede che l’innovazione non sia qualunque risultato del progresso tecnologico ma solo quello capace di accrescere il benessere collettivo.

E, naturalmente, il benessere collettivo non può essere il risultato del travalicamento e travolgimento dei diritti e delle libertà delle persone.

Ecco un’altra lezione.

Chi l’ha detto che bisogna scegliere tra progresso tecnologico e diritti?

Chi l’ha detto che esigere il rispetto dei secondi significa avercela con la prima e volerla frenare?

Non è così, non può esserlo e non deve esserlo.

Diritto a fare impresa, diritto a innovare, diritto alla protezione dei dati personali sono tutti tasselli irrinunciabili del patrimonio genetico della nostra democrazia e della nostra società.

È sbagliato per principio porre un cittadino, un imprenditore, un utente o un consumatore davanti a un bivio che

in realtà non esiste: da una parte il progresso e dall'altra i diritti e le libertà.

Non è quello che deve accadere.

E la storia di ChatGPT, in effetti, sembra raccontarlo in maniera plastica.

Perché quando si è ordinato a OpenAI la sospensione del trattamento dei dati personali, ci si è, in fondo, limitati a ricordare a una società commerciale americana nella quale una corporation del calibro di Microsoft aveva da poco investito oltre 10 miliardi di dollari e che in pochi mesi aveva raggiunto quasi 200 milioni di utenti che le regole, i diritti e le libertà vanno rispettati sempre e da tutti a prescindere da quanto sia "innovativo" il servizio che si offre, a prescindere dall'utilità che lo stesso può produrre per la società, a prescindere dal sacrosanto e legittimo perseguimento del diritto di fare impresa.

E non è stato un fatto di capricciosa applicazione di regole di dettaglio.

OpenAI ha addestrato i propri algoritmi – quelli sui quali si fonda il suo business e le straordinarie potenzialità dei suoi servizi – pescando a strascico, almeno online, miliardi di dati, anche personali, di miliardi di persone senza dir loro nulla e senza offrire loro neppure la possibilità di opporsi a questo trattamento coatto.

Una cosa che la disciplina europea, con poche eccezioni, non consente neppure a chi fa ricerca medica o scientifica.

Ma non basta perché ChatGPT, interrogata per il nome e il cognome di una persona, talvolta soffre di "allucinazioni" e associa a quella persona, fatti e circostanze non veritieri: di un professore americano, per esempio, ha detto che avrebbe sessualmente molestato una studentessa in Alaska senza che fosse mai andato in Alaska e, soprattutto, avesse mai molestato nessuno.

Sono cose capaci di distruggere letteralmente la vita di una persona.

Quale avrebbe dovuto essere e quale dovrebbe essere il ruolo dello Stato in tutte le sue articolazioni in casi come questi?

Farsi spettatore e lasciar fare al mercato?

Lasciare al mercato – a un mercato, peraltro, asfittico e oligopolistico come quello digitale – il compito di regolare sé stesso?

La sensazione, in tutta franchezza, è che rispondere affermativamente non sia possibile.

E che, ugualmente, sarebbe sbagliato suggerire un'antitesi e una contrapposizione che non c'è tra regole e progresso.

Questa contrapposizione non esiste e non può esistere sotto l'ombrello della nostra Costituzione che non ammette diritti tiranni e non consente quindi né al diritto alla privacy di fagocitare la libertà di impresa e quella a innovare, né a queste ultime di fagocitare il diritto alla privacy o altri diritti e libertà fondamentali.

La parola d'ordine in questi casi è bilanciamento.

E l'algoritmo di bilanciamento è sempre lo stesso: comprimere un diritto nella misura minima necessaria a garantire il rispetto e l'esercizio dell'altro.

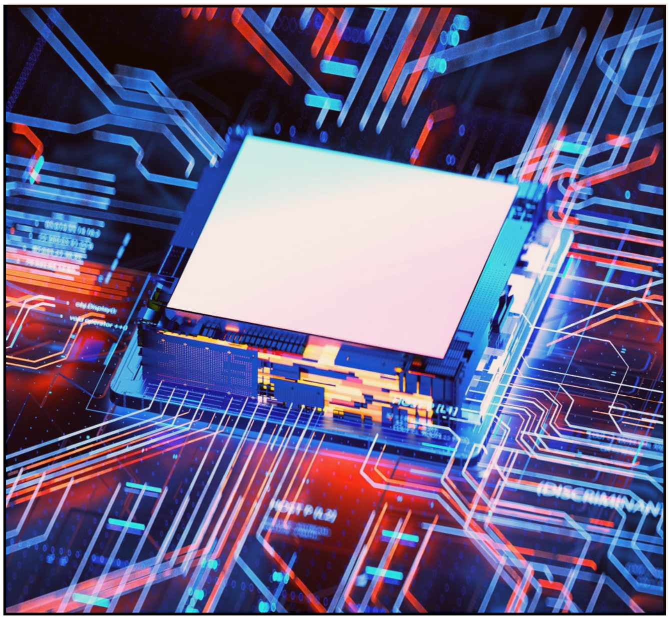
Ed è questo l'algoritmo che si è applicato: all'indomani del primo provvedimento si è aperto un confronto con OpenAI, si è capito fin dove la società potesse spingersi nell'immediato per conformarsi alla disciplina europea, si è imposta con un nuovo provvedimento una serie di correttivi e si è consentito alla società di tornare a rendere accessibile ChatGPT anche in Italia in attesa dell'attività istruttoria frattanto avviata.

Oggi il servizio è più trasparente e più rispettoso dei diritti e delle libertà delle personali anche se, forse, non abbastanza e di questo si discuterà nel corso del procedimento in corso.

Le regole, i diritti e le libertà possono e devono essere tradotti in vincolo tecnologico, devono orientare il progresso, plasmare e dare forma agli algoritmi, non vietare, bloccare o ostacolare ma guidare l'innovazione verso quella che dovrebbe sempre esserne la finalità ultima: massimizzare, accrescere e amplificare il benessere collettivo.

Ma come si fa a riuscire nell'impresa?

Nessuno, probabilmente - specie in una stagione come questa della vita del mondo in cui tutto scorre veloce, tutto cambia e si trasforma e l'imprevedibilità è l'unica certezza – ha la risposta ma il dialogo e il confronto interdisciplinare sembrano destinati a avere un ruolo essenziale nella ricerca di una soluzione.



Attacchi hacker e problemi di attribuzione

A cura di Ranieri Razzante

L'evoluzione tecnologica e le nuove frontiere della comunicazione hanno portato alla proliferazione di nuove condotte penalmente rilevanti, nonché ad una significativa espansione delle attività illecite - anche nel Metaverso, difficilmente controllabili [1].

Tra esse rientrano non solo gli, ormai comuni, attacchi informatici[2], bensì anche le operazioni svolte contro uno Stato[3].

Un esempio emblematico si rivede in quanto accaduto ad inizio 2023, a seguito della visita della Premier Meloni a Kiev.

Un importante attacco informatico, rivolto ad istituzioni ed imprese italiane, è stato messo in atto da un gruppo di hacker russi noto come NoName. Tra i siti attaccati ci sono stati quello dell'Arma dei Carabinieri, del Ministero degli Esteri e della Difesa, come anche quelli di società quali Tim, Banca Bper e Utility A2a.

I responsabili appartengono ad un collettivo di hacker vicino ai servizi segreti esteri russi – il Servizio di intelligence internazionale – i cui crimini, sofisticati e difficili da prevedere, vedono un nuovo allarmante livello di pericolosità[4].

Risulta evidente che, in tale contesto, la sfida cyber più ardua e delicata riguarda l'attribuzione, ovvero l'identificazione dei cyber criminali, autori di tali reati (cracker). L'espressione, che deriva dal termine hacker, è usata in accezione negativa per indicare coloro che possiedono avanzate capacità informatiche utilizzate al fine di commettere cyber attacchi.

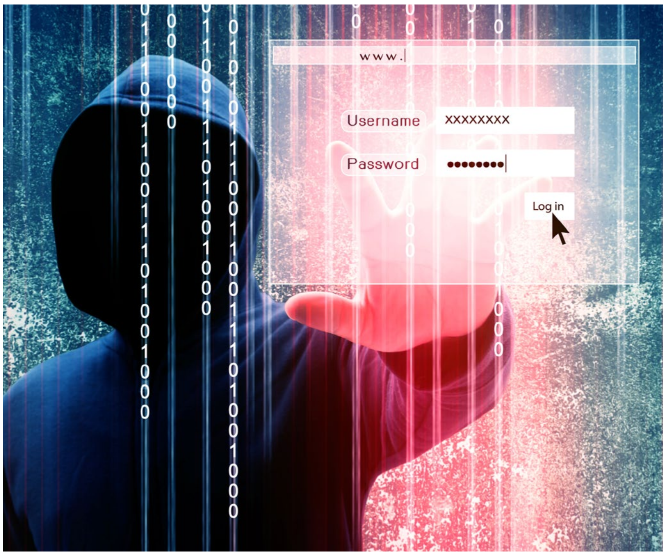
Invero, in base agli obiettivi nonché alle motivazioni che spingono tali attori ad agire, si riconoscono diverse tipologie di soggetti: quelli sponsorizzati dallo Stato, i criminali informatici, i cyberterroristi e, da ultimo, gli hacktivisti.

Nello specifico, quando si parla di cyberterroristi si intendono gruppi politici estremisti che utilizzano tecniche informatiche per realizzare attacchi tecnologici con lo scopo di intimidire, costringere o influenzare il pubblico, di provocare paura o causare danni fisici. Ciò anche grazie al darkweb, luogo di condivisione di informazioni, raccolta fondi, incontri e propaganda[5].

Dunque, la profilazione di questi ultimi risulta essere un'attività centrale se si vuole prevenire le mosse, comprendere le ragioni e l'origine degli attacchi e costruire strategie di difesa efficaci. Ciò avviene attraverso la raccolta di prove digitali e dati, spesso volontariamente offuscati dai responsabili. Questa operazione, per avere valore, deve necessariamente essere pubblica - e quindi credibile - al fine di legittimare giuridicamente una effettiva tutela[6].

Il processo di attribuzione, però, non è privo di insidie. Oltre alle difficoltà legate al panorama informatico e tecnico, vi sono due importanti problemi. In primo luogo, la scoperta degli avvenuti attacchi: a tale scopo, infatti, esistono indicatori di compromissione che rinvengono comportamenti anomali nei sistemi informatici ed effettuano controlli periodici.

In secondo luogo, quando si tratta di attacchi contro uno Stato, possono sorgere complicazioni di tipo politico. Nel diritto internazionale, l'art. 51 dello Statuto delle Nazioni Unite riconosce: «nel caso che abbia luogo un attacco armato contro un Membro delle Nazioni Unite (...) il diritto naturale di autotutela individuale o collettiva»[7]. Tuttavia, in merito alle contromisure, non vi è uno specifico consenso a livello di Nazioni Unite, per questo, vengono spesso applicate sanzioni quali blocchi dei conti, divieti di spostamento o denunce pubbliche dei comportamenti illeciti.



Invero, affinché si possa ritenere sussistente un illecito internazionale, è necessaria l'integrazione del relativo elemento oggettivo, il cui fondamento risiede nella violazione di un obbligo internazionale facente capo allo Stato.

A tal fine, potrebbe addursi come referente giuridico l'art. 2, par 4, della Carta delle Nazioni Unite, che dispone: «I Membri devono astenersi, nelle loro relazioni internazionali, dalla minaccia o dall'uso della forza, sia contro l'integrità territoriale o l'indipendenza politica di qualsiasi Stato, sia in qualunque altra maniera incompatibile con i fini delle Nazioni Unite».

Dunque, è possibile inquadrare tali cyber attacchi nel concetto di uso della forza, con conseguente applicabilità della legittima difesa di cui all'art 51 della Carta. Ammettendo tale soluzione, si riterrebbe integrato l'elemento oggettivo di un illecito internazionale, consistente nella violazione dell'obbligo giuridico avente ad oggetto il generale dovere di astensione dall'uso della forza[8].

Allo stato dei fatti, si comprende l'importanza del luogo di realizzazione di suddetti reati; soprattutto se si pensa al Metaverso. Difatti, essendo questo una realtà digitale, risultante dall'insieme di dimensioni virtuali e reali interconnesse, in cui gli utenti vengono rappresentati da propri alter ego - definiti avatar - questo nuovo mondo fa sorgere molti interrogativi in merito alla possibilità di applicarvi le tradizionali categorie del diritto[9], ponendo l'interprete davanti a questioni quali la perseguibilità di azioni ivi poste in essere, la relativa qualificazione e la possibilità di effettiva comminazione della pena.

Dal momento che le condotte realizzate sul web si estrinsecano nell'emanazione o nella captazione di una serie di impulsi elettronici, interconnessi tra loro, indifferentemente dalla concreta ubicazione del soggetto agente, il reato assume una connaturata ed inevitabile dimensione transnazionale, per cui l'attività di individuazione dei responsabili risulterà complessa. A tal proposito, ci si chiede se sia possibile ritenere che il Metaverso possa rappresentare un vero e proprio locus commissi delicti. Ciononostante, è ormai chiaro che una realtà diversa da quella fattuale è, oggi, idonea alla commissione di reati [10].

I principi e le competenze fondamentali al servizio della digital compliance

A cura di Andrea Lisi

Si chiede spesso al diritto di inseguire la tecnologia digitale che in questo periodo sta compiendo passi da gigante. E ogni novità, dall'intelligenza digitale alla blockchain sino al metaverso, si porta dietro insistite richieste di regolamentazione, perché i rischi che l'innovazione tecnologica porta con sé non sarebbero sostenibili e metterebbero in discussione la stessa nostra esistenza.

Lungi dal voler affrontare l'arduo compito di comprendere come le nuove tecnologie possano sconvolgere (in bene o in male) le nostre esistenze, mi limiterò a fornire una breve guida su come procedere in punto di diritto, in modo di evitare di chiedere al legislatore ciò che è bene che non faccia, così da consentire, magari, a professionisti preparati in ottica interdisciplinare di procedere con consapevolezza lungo i binari delle regolamentazioni già esistenti e tracciare finalmente un quadro solido per l'innovazione che vogliamo portare avanti per il nostro Sistema Paese. Effettivamente, come vedremo insieme, il diritto - a livello legislativo – deve e dovrebbe rimanere regolamentazione di fattispecie astratte, lasciando a noi interpreti il compito delicato di adattare alla realtà mutevole, che oggi caratterizza la nostra esistenza, i principi generali che si sono stratificati lungo centinaia di anni. E questo significherebbe sostanzialmente dare piena attuazione al fondamentale principio - di ispirazione common law - dell'accountability che contraddistingue le regolamentazioni europee più recenti in materia di mercati digitali e libera circolazione dei dati.

Elemento dirimente per noi professionisti, attenti interpreti di una realtà che sta vertiginosamente cambiando, è comprendere come vadano correttamente usate le risorse che abbiamo a disposizione e in queste rientra senz'altro l'evoluzione tecnologica. Ciò nell'ottica di non scivolare e magari rovinare in adempimenti ad uso esclusivamente burocratico.

I rischi insiti nello sviluppo di tecnologie digitali

Ovviamente la realtà digitalmente mutevole che riguarda noi tutti va osservata con attenzione per poter essere con pazienza regolamentata in modo concreto e proattivo. E, ciò che oggi è certo, è che qualsiasi direzione - più o meno metaversica e più o meno intelligente - dovesse prendere la tecnologia digitale, il cuore pulsante dell'evoluzione sarà costituito dalla gestione di enormi database profilatissimi in modo compatibile con i nostri diritti fondamentali. Quindi, in una società evidentemente datificata, assicurare la pienezza del valore alle proprie informazioni digitali dovrebbe risultare un'ovvietà per qualsiasi ente (pubblico o privato). Appare pertanto inevitabile, per chi si occupa di sviluppare dei processi innovativi, avere come fine ultimo di ogni sua azione il perseguimento costante dei principi della security e della privacy by design (e by default).

Del resto, avere in pancia del proprio sistema aziendale dati e informazioni manipolabili e accessibili a chiunque credo che oggi non convenga a nessuno e rischierebbe di compromettere il valore di qualsiasi processo di digitalizzazione, oltre che incrinare irrimediabilmente la propria reputation. Infatti, come ribadisce il considerando 75 del GDPR (Regolamento (UE) 2016/679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati), qualsiasi trattamento di dati personali può comportare rischi specifici per gli interessati a quei trattamenti[11]. E la possibile esposizione a specifici rischi per i diritti e libertà degli interessati comporta, per qualsiasi ente che sviluppa progetti di innovazione digitale, una particolare e indispensabile attenzione alla compliance normativa in materia IT, salvo rischiare di esporsi a pesantissime sanzioni e/o richieste di risarcimento danni da parte di interessati violati nei loro diritti e libertà fondamentali.

Il valore del dato

Per qualsiasi ente pubblico o privato è quindi oggi indispensabile perseguire strategie organizzative per gestire e custodire i propri dati. Garantire la qualità, la corretta accessibilità, l'interoperabilità, l'integrità, l'immodificabilità, quindi, la sicurezza e l'autenticità al proprio patrimonio informativo è fondamentale: raggiungere un modello corretto di compliance sui propri dati (personali e non) deve entrare così nelle corde di qualsiasi società o pubblica amministrazione. Vanno, pertanto, governati e custoditi i propri dati rilevanti, attraverso accurate analisi del rischio che assicurino adeguate misure di sicurezza a protezione di ogni asset informativo.

Le registrazioni affidabili costituiscono, del resto, i documenti del nostro presente digitale ed essi possono essere assicurati nel loro valore solo da un corredo di metadati che abbia una logica anche archivistica. E per un qualsiasi ente gli stessi data breach - ormai entrati prepotentemente nella cronaca dell'ultimo periodo - non possono essere valutati solo come personal data breach, così come i DPO (Data Protection Officer e Digital Preservation Officer) devono trovare un ruolo che sia di presidio complessivo del patrimonio informativo pubblico o privato.

L'accountability nella gestione efficace di database e archivi digitali

Nella necessaria tutela dei propri patrimoni informativi e documentali si intersecano normative diverse con obiettivi ultimi spesso coincidenti. In particolare, i principi di esattezza, affidabilità, integrità, immodificabilità, autenticità, trasparenza e accessibilità riecheggiano nelle normative generali che regolamentano la materia, come il Codice dell'amministrazione digitale (che si occupa proprio di delineare i presidi fondamentali della gestione e conservazione del proprio patrimonio informativo e documentale), o il già citato GDPR (in materia di protezione dei propri database) e il D. Lgs. 33/2013 (su open data, trasparenza e pubblicità legale online). A queste normative andrebbero aggiunti i vari regolamenti europei in vigore che oggi si occupano di delineare un quadro uniforme per favorire lo sviluppo dei mercati digitali.

Per concretizzare tali principi occorre predisporre quindi processi, metodologie e regole per un records management che sia finalizzato a mantenere custodito nel tempo il contesto di dati (anche strutturati), informazioni e docu-

menti (anche e soprattutto nativi) digitali rilevanti per gli enti pubblici e privati attraverso altresì una regolamentazione contrattuale consapevole. E per raggiungere tali obiettivi non occorre partire dalla scelta tecnologica (scelta che deve essere invece l'esito di una valutazione ponderata e responsabile), ma è indispensabile operare delle costanti verifiche sulla propria compliance legale e organizzativa, quindi dedicarsi a definire con attenzione competenze, ruoli e responsabilità interdisciplinari, prima dell'avvio di qualsiasi progetto con impatto digitale.

Come garantire la digital compliance?

La digital compliance è un processo a tappe, di trasparente mappatura, prima di tutto, e che comporta una visione a 360° tra discipline diverse in grado di presidiare materie così complesse e affascinanti. Infatti, i vari documenti e contratti che le diverse discipline normative prevedono (e che corredano l'accountability dei processi di digitalizzazione) devono a loro volta "parlarsi tra loro". E tali documenti devono quindi essere frutto di una coordinata mappatura e un'analisi del rischio portate avanti da team interdisciplinari, come appunto la normativa prevede.

La necessità di favorire lo sviluppo di team interdisciplinari per poter cavalcare l'innovazione digitale

Progetti che perseguano l'assioma del "Digital First" hanno bisogno di interdisciplinarità, quindi di "interferenze" tra professionalità molto diverse che siano capaci di confrontarsi su obiettivi comuni, focalizzandosi su una corretta mappatura sia dei flussi informativi e documentali e sia dell'intera organizzazione (fatta di tecnologie e risorse umane) a presidio degli stessi. Da tale trasparente mappatura si può ricavare una verifica puntuale delle soluzioni applicative, anche per assicurare una coerente applicazione dei (tante volte citati) principi della privacy by design e della privacy by default, come individuati nell'art. 25 del GDPR. In particolare, secondo il considerando 78 del GDPR "in fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali per svolgere le loro funzioni, i produttori dei prodotti, dei servizi e delle applicazioni dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni e, tenuto debito conto dello stato dell'arte, a far sì che i titolari del trattamento e i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati. I principi della protezione dei dati fin dalla progettazione e di default dovrebbero essere presi in considerazione anche nell'ambito degli appalti pubblici".

In estrema sintesi, la tecnologia rimane uno strumento indispensabile di sviluppo per aziende pubbliche e private, ma per essere volano di crescita, senza rischiare di calpestare diritti e libertà fondamentali, ha estremo bisogno di presidi organizzativi in grado anche di dare concretezza e documentare in modo affidabile alcuni principi fondamentali su cui si fonda oggi il nostro intero ordinamento giuridico.

CYBER
Think Tank
ASSINTEL

Cyber Think Tank Assintel

Connessioni che fanno la differenza. Se non sei socio, associati!

Progetti 2023:

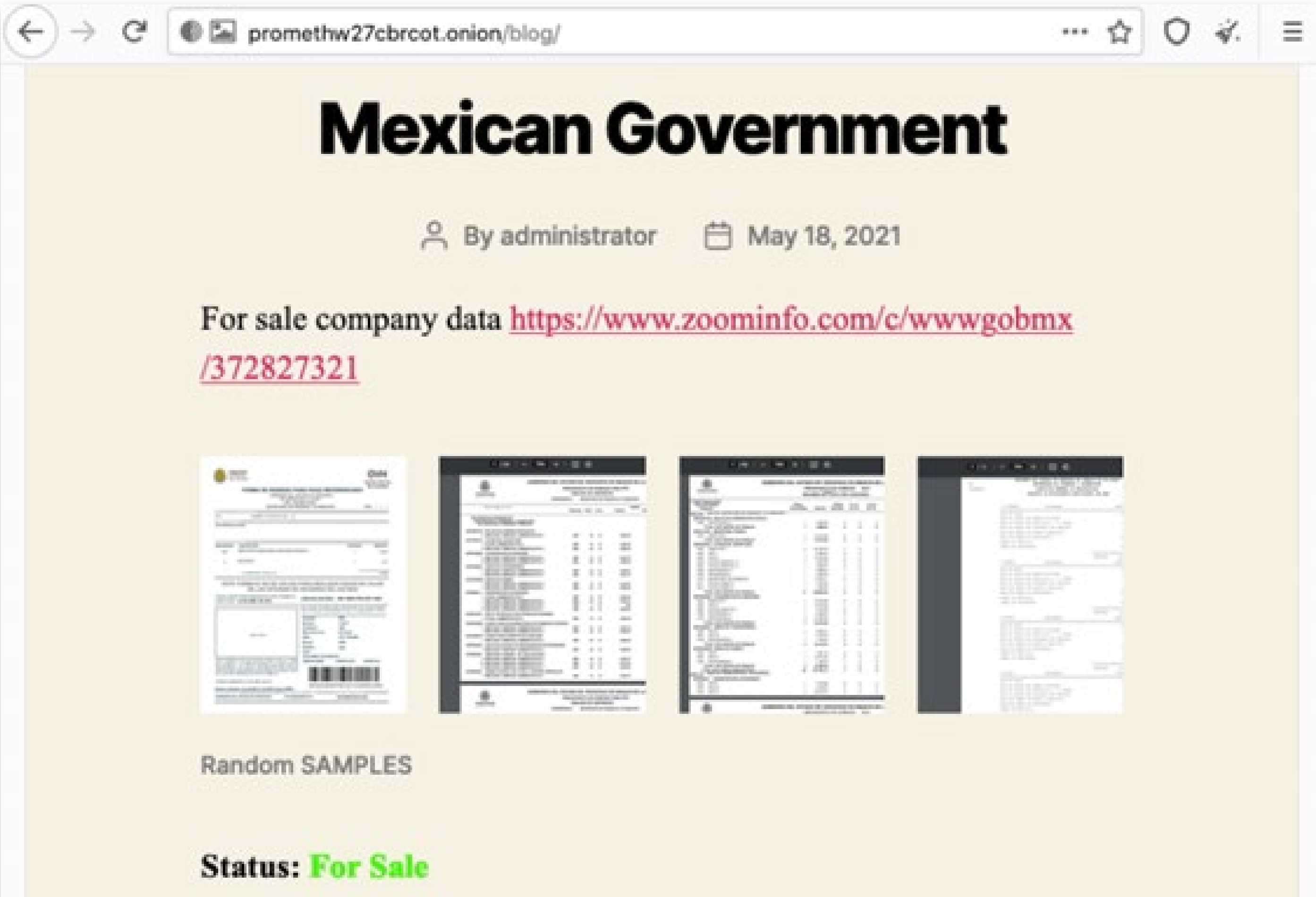
1. Magazine
2. Webinar
3. Assintel Cyber Hub
4. Threat Infosharing

Per info scrivi a:

segreteria@assintel.it

Prometheus: una nuova comparsa sulla scena del ransomware

A cura di Selene Giupponi



Il gruppo Prometheus ha messo in vendita dati di 27 vittime, comprese informazioni appartenenti ad agenzie governative messicane.

I ricercatori della compagnia di cybersecurity Resecurity (basata a Los Angeles) hanno scoperto due nuovi gruppi ransomware – Prometheus e Grief. In questo articolo prenderemo in considerazione il primo.

Prometheus

Il gruppo emergente di ransomware Prometheus ha fatto notizia il mese scorso con il rapporto di Unit42. Secondo il rapporto, che ha osservato Prometheus per 4 mesi, le vittime del gruppo emergente di ransomware ammontano a più di 30 in più paesi diversi, tra cui Stati Uniti, Regno Unito e una dozzina di altri paesi in Asia, Europa, Medio Oriente, e Sud America.

Le organizzazioni prese di mira dagli attacchi di Prometheus includevano agenzie governative, servizi finanziari, produzione, logistica, agricoltura, servizi sanitari, agenzie assicurative, energia, consulenza, studi legali e altro ancora.

Sebbene Prometheus abbia affermato di essere affiliato a REvil (il gruppo di ransomware con sede in Russia attribuito all'attacco al fornitore globale di carne JBS che è riuscito ad ottenere un riscatto di 11 milioni di dollari, il codice e il comportamento di Prometheus sono più simili a Thanos.[12]

Alcuni dei campioni di malware associati a Prometheus sono stati rilevati da popolari motori antivirus, come ad esempio il ransomware Thanos (noto anche come Hakbit), sostengono gli esperti.

Thanos[13] fu sviluppato dal gruppo Nosophoros, che vende malware nelle comunità underground.

Sebbene il Thanos originale non sia così attivo, il suo codice non riposa[14]: a metà del 2021 è stato rilevato in ulteriori attacchi ransomware, questa volta utilizzati da un gruppo chiamato “Haron”.

Lo stesso codice Thanos era ed è utilizzato da più attori di minacce, alcuni dei quali sospettati di avere legami sponsorizzati dallo stato-nazione. La variante Prometeo si è estinta negli ultimi mesi, ma altre varianti possono continuare a sorgere dalla stessa base Thanos. Ciò che cambia attraverso ogni variazione è la personalizzazione. Nel caso di Prometheus, i suoi operatori usavano bene l’ingegneria sociale, ma non erano così abili nel lavorare con la crittografia.

Il gruppo ha utilizzato Sonar, uno strumento di trasferimento dati sicuro integrato nella rete Tor e che fornisce un’API, secondo Resecurity [15].

Il gruppo passa quindi a un sistema di biglietteria automatizzato in cui le vittime possono fornire i propri ID e pagare in criptovalute BTC o XMR per un’ulteriore decrittazione[16] .

La vulnerabilità SQL del sito di leaks di Prometheus, incorporato in TOR, ha consentito la divulgazione degli indirizzi e-mail degli operatori. Quindi i partecipanti alla minaccia scoprono e correggono le vulnerabilità.

Stranamente, alcuni casi identificati con gli esercizi di Prometeo o Prom (nome alternativo) possono essere rilevati dai principali motori antivirus come Thanos ransomware. Il ransomware Thanos (altrimenti chiamato programma Hawkbit Rank) è stato creato da Nosophoros, un estremista clandestino che lo ha offerto a reti nel dark web. Ha anche lavorato con alcuni donatori promuovendo il ransomware Jigsaw e vendendo accessi RDP e VPN scambiati ad altre organizzazioni, incluso il rullo di tamburi, come affermato da Resecurity[17] e KELA[18]. Hanno resoconti completi dei loro esercizi segreti nel Dark Web[19] .

Come funziona

Prometheus ransomware utilizza il cifrario salsa20 con una password casuale basata su tickcount per la crittografia. La dimensione della password casuale è di 32 byte e ogni carattere è un carattere visibile. Poiché la password utilizza il tickcount come chiave, è possibile conoscerla attraverso tentativi brute force.

La società di sicurezza taiwanese CyCraft ha rilasciato un’applicazione gratuita che può aiutare le vittime del ransomware Prometheus a recuperare e decrittografare alcuni dei loro file.

Disponibile su GitHub,al seguente link (https://github.com/cycraft-corp/Prometheus-Decryptor) il decryptor funziona efficacemente forzando la chiave di crittografia utilizzata per bloccare i dati della vittima.

Come rompere Prometeo

Mentre lavoravano sui campioni Prometheus che crittografavano i file sui dispositivi infetti, alcuni ricercatori hanno scoperto un punto debole nell’algoritmo di generazione delle chiavi utilizzato nel processo di crittografia. A differenza della maggior parte dei casi di ransomware, questa è stata una buona notizia che ha finito per aiutare un’organizzazione vittimizzata.

La nostra analisi ha dimostrato che per generare il seme per la crittografia, l’algoritmo selezionato da Prometheus utilizza un vettore di inizializzazione codificato (IV) e il tempo di attività del computer. Ciò significa che il valore di inizializzazione è molto più facile da indovinare di quanto dovrebbe essere, poiché è possibile ottenere determinati parametri relativi al file crittografato e al dispositivo infetto.

Sulla base di tali parametri, X-Force ha scritto un decryptor che ha finito per funzionare rapidamente per decrittografare i tipi di file che avevano intestazioni di file note, ad esempio: pdf, doc, xls, ppt, docx, xlsx, pptx, 7z, mp3, jpg, jpeg, zip, iso, exe, dll, sys e png. La decrittazione dei file è stata resa ancora più semplice quando era noto il tempo di avvio del dispositivo. I tempi di avvio non sono un parametro che si dovrebbe indovinare, possono essere ottenuti tramite il file CBS.log nella directory di

Windows.

L'utilizzo del decryptor è stata un'ottima opzione per il processo di recupero supportato da X-Force, ma qui è importante un'altra nota. Alcuni strumenti di decrittazione open source possono emergere nel tempo e potrebbero sembrare uno strumento di recupero che può aiutare in casi su larga scala. Bisogna considerare il tempo necessario a un decryptor per sbloccare ogni file. Alcuni strumenti open source possono richiedere circa cinque ore per file o più, il che richiederebbe troppo tempo nei casi in cui molti dati non sono più accessibili. Una ragionevole quantità di tempo per decrittografare ogni file dovrebbe essere di pochi minuti o meno.

Metodologia di crittografia e debolezze

Nelle varianti di Prometheus analizzate, ci sono due modi in cui il ransomware può essere configurato per la crittografia:

Metodo n. 1:

1. Una stringa di 32 byte viene generata utilizzando la classe Random di C#. Viene utilizzato il costruttore predefinito, che passa Environment.TickCount come seme;
2. La stringa viene quindi crittografata utilizzando una chiave pubblica RSA hardcoded. Viene utilizzato il riempimento PKCS#1 v1.5. Il testo cifrato viene quindi codificato Base64;
3. Il file viene crittografato utilizzando un algoritmo simmetrico (Salsa20) con un array di 8 byte codificato come vettore di inizializzazione (IV);
4. La chiave è la stringa di 32 byte descritta sopra. Il testo cifrato viene scritto nel file crittografato;
5. La chiave crittografata con codifica Base64 viene quindi aggiunta alla fine del file crittografato, insieme alla stringa "GotAllDone".

Metodo n. 2:

1. Una stringa di 32 byte viene generata utilizzando la classe Random di C#. Viene utilizzato il costruttore predefinito, che passa Environment.TickCount come seme;
2. La stringa viene quindi crittografata utilizzando una chiave pubblica RSA hardcoded. Viene utilizzato il riempimento PKCS#1 v1.5. Il testo cifrato viene quindi codificato Base64;
3. RFC2898DeriveBytes viene utilizzato per generare una chiave a 32 byte e un IV a 8 byte. La classe Rfc2898DeriveBytes implementa la funzionalità di derivazione della chiave basata su password, PBKDF2, utilizzando un generatore di numeri pseudo-casuali. La stringa generata in precedenza viene utilizzata come password e il salt è un array di 8 byte codificato;
4. Il file viene crittografato utilizzando un algoritmo simmetrico utilizzando i parametri generati sopra. Il testo cifrato viene scritto nel file crittografato;
5. La chiave crittografata con codifica Base64 viene quindi aggiunta alla fine del file crittografato, insieme alla stringa "GotAllDone".

Debolezze in questa metodologia di crittografia.

Gli analisti hanno riscontrato che questa tecnica mancava di un modo che consentisse di trovare un modo per decrittografare i file interessati.

La classe Random di C# genererà esattamente gli stessi byte purché il seme sia noto. In questo caso, il seme è la variabile Environment.TickCount, ovvero il numero di millisecondi trascorsi dall'ultimo avvio di un computer.

Quel valore seme può essere indovinato dati determinati parametri. Inoltre, anche la variabile Environment.TickCount viene aggiornata circa ogni 16 millisecondi, quindi è possibile che più file abbiano la stessa chiave, il che può rendere la decrittazione ancora più veloce lungo la linea.

L'IV hardcoded non ha fornito alcuna sicurezza aggiuntiva in questo caso, considerando che può essere facilmente ottenuto e sembra essere lo stesso per ogni campione analizzato. Per rendere più forte la crittografia, l'IV dovrebbe essere in genere casuale o pseudocasuale.

Requisiti e problemi di decrittazione

L'analisi dei ricercatori indica che qualsiasi campione di Prometheus che utilizza la classe C# Random per generare chiavi è vulnerabile. Da notare, hanno decrittografato solo i file che sono stati crittografati utilizzando un cifrario a flusso Salsa20. Alcuni campioni di ransomware Prometheus possono essere configurati per utilizzare AES-256 e sebbene questi campioni siano ancora vulnerabili, i ricercatori non hanno testato il decryptor su tali campioni nel loro lavoro attuale.

Il modello di resilienza europea nella strategia di integrazione tra cyber e spazio

A cura di Davide Maniscalco

L'evoluzione del cosiddetto quinto dominio, ovvero quello cibernetico, lo ha reso sempre più ingerente ed interconnesso con il dominio tradizionale dello spazio.

Ed invero, l'ecosistema spaziale è caratterizzato dalle interrelazioni tra le infrastrutture di terra e di lancio, e dai relativi collegamenti in radiofrequenza, con i sistemi orbitali e la fornitura dei relativi servizi dell'industria spaziale nell'UE e negli Stati membri.

In tale complesso e strategico ecosistema dinamico, la minaccia cibernetica si sta sviluppando attraverso una serie di attività ostili intenzionali preordinate ad ottenere e/o capitalizzare un vantaggio informativo riveniente dallo sfruttamento di vulnerabilità dei sistemi spaziali infrastrutturali ed orbitali dual use.

Del resto alcune potenze spaziali hanno dimostrato, anche di recente, le loro potenziali capacità di colpire le infrastrutture spaziali critiche, peraltro investendo e testando tecnologie anti-satellite particolarmente disruptive dei sistemi e servizi spaziali.

Ne consegue che il dominio spaziale e quello cibernetico dovranno sempre più integrarsi per favorire una sempre maggiore autonomia strategica dell'UE e dei suoi Stati membri, senz'altro funzionale alla crescita dell'economia data driven ma anche necessaria a migliorare la capacità di rilevare, caratterizzare e attribuire una minaccia nel dominio spaziale e di reagirvi in maniera tempestiva, proporzionata e coerente, sia a livello nazionale che dell'UE.

Per questa ragione, anche con le recenti revisionate Direttive europee CER, sulla resilienza dei soggetti critici, e NIS2 sulla sicurezza informatica, il Legislatore europeo ha individuato lo spazio come un dominio strategico dello Stategic Compass ed ha espressamente richiesto l'elaborazione di una strategia spaziale dell'UE per la sicurezza e la difesa, in grado assicurare un elevato livello di protezione e resilienza alle infrastrutture spaziali, da intendersi come servizi essenziali di un Paese, che debbono essere capaci dunque di rispondere a qualsiasi attività o minaccia ostile.

In tale chiara direzione va, infatti, la strategia europea spaziale per la sicurezza e la difesa che, pubblicata lo scorso 10 marzo con la comunicazione congiunta del-

la Commissione europea e dell'Alto Rappresentante dell'Unione per gli Affari Esteri e la Politica di Sicurezza, dimostra l'impegno dell'UE a proteggere i propri interessi di sicurezza evitando nel contempo una corsa agli armamenti nello spazio extra-atmosferico e accelerando le sinergie tra lo spazio, la sicurezza e la difesa.

Tuttavia, nelle more di una auspicabile armonizzazione regolatoria europea, l'approccio dell'UE potrebbe ricalcare quello delle citate Direttive, attraverso l'individuazione da parte degli Stati membri dei sistemi e i servizi spaziali essenziali in modo da costituire un "perimetro" di tutti i players coinvolti nelle relativa supply chain, introducendo conseguentemente un framework comune di requisiti di cybersecurity by design e di resilienza dei sistemi spaziali che offrono servizi essenziali e, parallelamente, lo sviluppo di piani nazionali coordinati di preparazione e resilienza nonché di protocolli di emergenza.

Appare evidente che siffatto approccio, potrebbe creare le condizioni, sia per lo sviluppo di centri di monitoraggio, sia per replicare il sistema di notifica degli incidenti sistemici su larga scala.

La realizzazione di tale modello passa inevitabilmente per l'istituzione e l'integrazione, in coerenza con la strategia europea per la cybersecurity, dello European

Cyber Shield, vale a dire di uno "scudo cibernetico europeo" che opererà su tre livelli di sicurezza: preventiva, proattiva e predittiva, al precipuo scopo di proteggere, rilevare, difendere e scoraggiare gli attori malevoli.

Lo scudo europeo richiederà ancora una volta l'affermazione della sovranità tecnologica europea al fine di affrancare gradualmente l'Europa dalle dipendenze informatiche e proiettarla, con ambizione di leadership digitale, nello sviluppo delle nuove tecnologie, sia in ambito civile sia in ambito militare.

L'attività di monitoraggio funzionale allo scambio di informazioni diventa così essenziale e, in tale scenario, la rete dei SOC federati e pertinenti potrà così integrare il Cyber Shield, sostenuto da una infrastruttura di rilevamento europea, con il sistema di monitoraggio ed analisi del dominio spaziale, realizzando compiutamente l'action plan europeo.

La vera sfida europea consiste infatti nello sviluppo di capacità, politiche, normative, tecniche ed operative, che consentano una rilevazione tempestiva degli attacchi cibernetici, attraverso un monitoraggio continuo della rete da parte dei SOC federati e pertinenti, con l'utilizzo di sistemi di intelligenza artificiale.

Sarà dunque importante puntare sul partenariato pubblico-privato al fine di promuovere una visione comune di comportamenti pacifici e responsabili nello spazio, rispondere alle minacce spaziali e sostenere l'utilizzo di servizi spaziali per la sicurezza e la difesa, in grado di assicurarne un elevato livello di innovazione in un contesto di sempre maggiore competitività dell'industria spaziale.

A tal riguardo, già nella Direttiva NIS2, da una lettura del Considerando 44, è possibile evincere una strategia che punta su una capacità di tempestiva rilevazione, ponendo peraltro enfasi sui cosiddetti Managed Security Service Providers (MSSP), nelle seguenti aree:

- incident response;
- penetration test;
- audit di sicurezza;
- consulenza (funzionale alla valutazione del rischio).

La Direttiva prevede infatti che i CSIRT dovrebbero avere la capacità, su richiesta di un soggetto essenziale o importante, di monitorarne le risorse esposte, sia in loco che a distanza, per identificare, comprendere e gestire i rischi organizzativi generali del soggetto con riguardo alle compromissioni della catena di approvvigionamento, ovvero alle vulnerabilità critiche.

Pertanto, il soggetto critico sarà incoraggiato a comunicare al CSIRT se gestisce un'interfaccia gestionale privilegiata poiché ciò potrebbe incidere sulla velocità delle azioni di mitigazione.

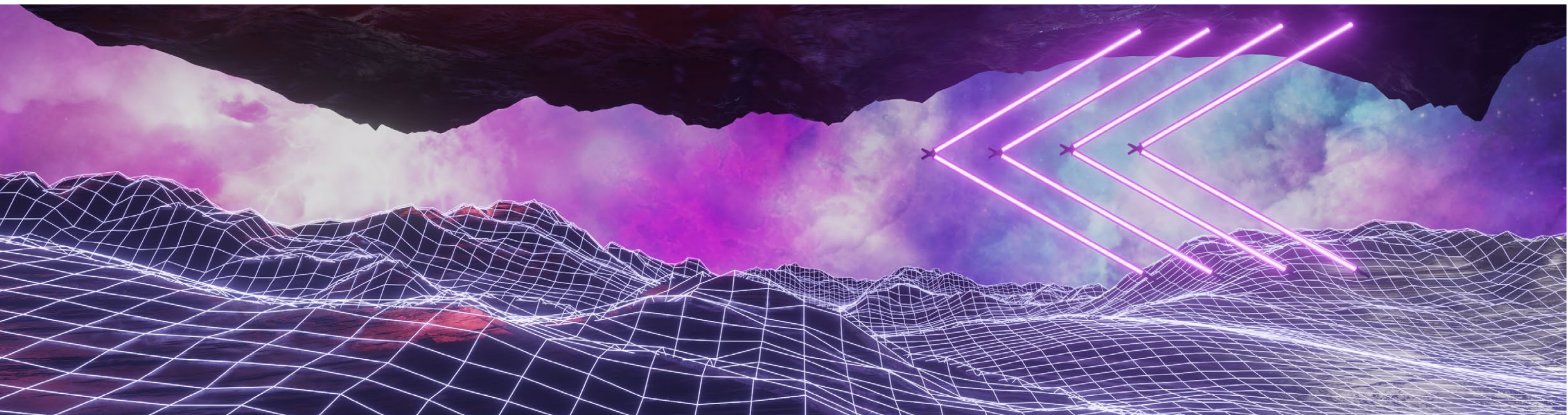
Ciò evidentemente richiede un rafforzamento del layer di sicurezza preventiva delle infrastrutture critiche, nell'ambito di regolari esercitazioni a livello europeo ed anche attraverso la fondamentale condivisione delle informazioni al fine di:

- testare, sviluppare e convalidare la risposta dell'UE alle minacce spaziali;
- testare ed esplorare meccanismi di solidarietà concreti in caso di attacchi dallo spazio o di minacce ai sistemi spaziali;
- sviluppare sinergie con i partner e gli alleati per la sicurezza e la difesa dello spazio.

In conclusione, se da un lato, l'attività normativa e regolatoria del dominio spaziale è ancora eterogenea e necessità di un'attività di armonizzazione in un quadro europeo, l'Europa può certamente già considerarsi una potenza spaziale globale, potendo attualmente vantare la gestione di risorse spaziali strategiche per il posizionamento, la navigazione e il cronometraggio, nonché per l'osservazione della Terra.

A ciò si aggiunga il già preannunciato lancio della Union Security Connectivity Program, vale a dire una terza costellazione per le comunicazioni satellitari sicure che garantirà un accesso continuo a livello globale a servizi di comunicazione altamente resilienti a cui si aggiungeranno ulteriori servizi a valore aggiunto come l'anonimato dell'uso, la bassa latenza e la flessibilità.

Inoltre, gli Stati membri possiedono e gestiscono già risorse spaziali nazionali, comprese le risorse che servono a scopi di sicurezza e difesa ed il Centro satellitare dell'UE fornisce una esclusiva capacità di analisi dell'intelligence geospaziale necessario a supportare il processo decisionale.



CYBER
Think Tank
ASSINTEL

LA SICUREZZA INIZIA CON TE, SE NON SEI SOCIO, ASSOCIATI E UNISCITI A NOI!

CYBER THINK TANK ASSINTEL

Per info scrivi a:

segreteria@assintel.it

AI – Domande e risposte facili facili

A cura di Gianpiero Cozzolino

Ciao, cos'è per te l'intelligenza artificiale?

"Intelligenza", analizzando la parola partendo dal nostro caro latino, mi vengono in mente INTUS e LEGERE, che a mio avviso portano alla definizione o traslazione temporale di LEGARE LE COSE, quindi potrei affermare che l'AI sia quel sistema non umano che sappia legare le cose.

Ma partiamo con il dire che cosa non è AI in modo da essere semplici: quasi tutta la robotica non è AI in quanto non si auto istruisce (anche se ha forma più o meno umana e "parla"...), così come anche tutti gli algoritmi "statici", cioè che compiono calcoli, per quanto complessi; per esempio il navigatore che abbiamo in auto, o una automobile a guida automatica non è munita di AI, eppure conosce i segnali stradali, conosce le regole di guida stradale, tiene la destra a Roma e la sinistra a Londra, sorpassa quando l'altra corsia è libera ed è permesso dal codice stradale, e se il calcolo fra velocità tempo e spazio lo permetta in sicurezza.

Si può dire che l'AI è quando un sistema automatico non ha un comportamento predeterminato e certo, secondo criteri decisi dal suo programmatore, ma al contrario il suo comportamento deriva da una sorta di "esperienza", cioè apprendimento su un insieme di dati. Al variare dei dati con cui il sistema viene istruito, varia anche il risultato delle elaborazioni richieste.

Per fare un esempio, prendendo la stessa automobile di prima e dotandola di AI, l'auto potrebbe iniziare a valutare se sia conveniente sorpassare, utilizzando man mano più dati, anche quelli che a nostro vedere forse non sarebbero necessari aggregare (non parlo dei dati meteo o del tipo di drenaggio dell'asfalto ma parlo dell'appuntamento della sera per andare a teatro); cerco di essere più facile per far emergere le differenze: la nostra UI (intelligenza umana) riesce ad aggregare molteplici fattori fisici come: velocità, umidità, temperatura, posizione, etc... fino ad un numero finito di fattori e valori che riusciamo ad aggregare e calcolare a "mente", ma poi entrano in campo anche altri fattori tipo quelli psicologici morali ed etici. Esempio facile: ma che bella canzone alla radio, mi ricorda quel pezzo rock di Elvis che ballavo in balera quando ho conosciuto la mia futura moglie, andavo alla grande, e vivevo la vita al massimo, sorpassando ogni difficoltà con la mia giovinezza, voglio riprovare quell'ebrezza... quindi aumenta in me la voglia di sorpassare ed invece di usare un poco di acceleratore e controllare due volte lo specchietto, scalo una marcia affondo il piede sul gas e vado! Cosa farà invece l'auto dotata di AI? Man mano (velocità di calcolo per una AI) avrà a disposizione sempre più dati così da sembrarci autonoma nelle decisioni e quel bel sorpasso con la radio a tutto volume forse non sarà mai eseguito, in quanto il semaforo che incontreremo sarà rosso, e la vettura che ci precede girerà a destra fra solo 30 mt.

Come ci aiuta o aiuterà?

I sistemi di AI non sono una novità: vengono studiati da decenni, ma sono diventati di uso comune grazie agli avanzamenti tecnologici che hanno aumentato le capacità di calcolo e di memorizzazione riducendo contemporaneamente i costi. Di conseguenza, esistono già delle applicazioni di uso abbastanza diffuso: gli esempi più comuni di sistemi che usano l'AI sono: il riconoscimento ed il comando vocale (come quello negli assistenti personali sugli smartphone o nelle auto); la scrittura di testi in risposta ad alcuni criteri sul contenuto; creazione e manipolazione di immagini (foto e video) come il restauro o il deep fake (cioè la sostituzione di un volto con un altro); il riconoscimento biometrico (utile per autenticazioni forti); il supporto alla sintesi di nuovi materiali o farmaci.

Per il futuro, si parla molto dei sistemi di diagnostica per immagini, che possono aiutare (mai sostituire) i medici, o le cosiddette città "smart" in cui gli spostamenti potrebbero essere ottimizzati sulla base della situazione in tempo reale delle strade e della guida automatica dei veicoli.

Di cosa ci dobbiamo preoccupare?

Due sono gli elementi di cui tenere conto.

Il primo è la scelta dell'insieme di dati su cui viene eseguito l'apprendimento, e che determina profondamente il comportamento successivo: se i dati sono sbagliati, incompleti, basati su pregiudizi, allora il risultato delle elaborazioni sarà sbagliato, incompleto, pregiudizievole.

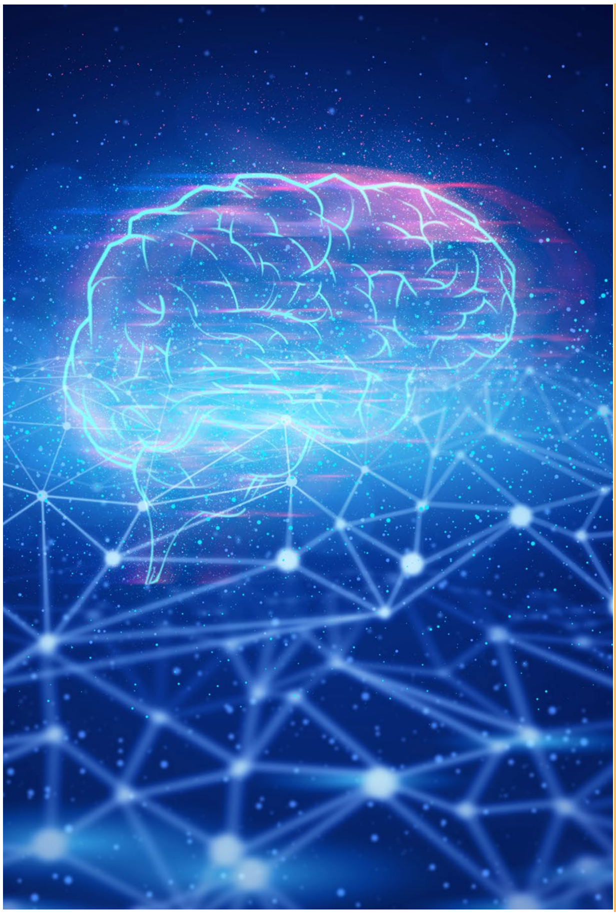
Il secondo è che, per come sono strutturati i sistemi di AI, i loro risultati non sono né prevedibili, né spiegabili a posteriori; significa che le decisioni eventualmente prese sulla base di questi risultati non sono controllabili né contestabili, poiché nessuno è in grado di spiegare come sono stati ottenuti.

Un esempio di questi rischi sono i sistemi di riconoscimento facciale utilizzati negli Stati Uniti dalle forze di polizia, che sono risultati poco affidabili soprattutto nei confronti delle persone di colore, per via di un insieme di dati scelto non correttamente e con criteri influenzati da un pregiudizio di fondo; un altro è la facilità con cui si possono generare false prove di notizie ovviamente false, contribuendo alla disinformazione ed alla propaganda.

In sostanza, il problema è che quando i sistemi di AI vengono usati per utilizzi che hanno conseguenze significative sulle persone, esse non sono in grado dal punto di vista tecnico di opporsi a tali conseguenze; ed infatti, la tutela può essere mantenuta solo a livello giuridico, come infatti sta avvenendo nella legislazione europea (per esempio nella normativa sulla protezione dei dati personali e sulla normativa specificatamente dedicata all'AI).

Non a caso, da molte parti si chiede un approccio etico ai sistemi di AI, cioè che dia priorità all'utilità per il progresso umano e non ai soliti interessi economici o puramente tecnologici.

Faccio il solito esempio facile facile così da comprendere lo stato della situazione, non entro in merito all'etica della vita umana: oggi la diagnostica per immagini è supportata da moltissima tecnologia fisica e matematica, per cui prendiamo per esempio una ecografia su di un feto di 12 settimane, il feto dovrebbe avere una dimensione tra i 5 e i 6 centimetri, la ginecologa utilizza poi l'ecografo tarandolo in maniera adeguata per vedere meglio le morfologie ed altri 1000 dati che ha studiato ed imparato nel corso dei suoi studi, e nel periodo di specializzazione ed del suo esercizio della professione. L'ecografo tramite matematica e fisica cerca di restituire un rendering sempre migliore; se diamo valore 1000 alle capacità di analisi della Dottoressa, domani con l'ecografo dotato di AI i parametri controllati potranno essere 100'000, aggregando per esempio i dati storici clinici di tutto il DNA legato al feto, partendo dal bisnonno nato nel 1998 e della bisnonna nata nel 2003. In questi 100'000 check ce ne sarà sicuramente qualcuno negativo, che pregiudicherà la gravidanza o la vita futura, quindi se l'essere calvi a 50 anni non sarà di moda, l'AI sconsiglierà di proseguire la gravidanza e metterà agli atti che a suo GIUDIZIO il feto non è conforme agli "standard" qualitativi, mentre la dottoressa potrà dire: tutto procede per il meglio, attendiamo l'ecografia della 18ma settimana per vedere il sesso, stai tranquilla e goditi questa esperienza meravigliosa.



Blockchain e Sanità: un connubio perfetto per la tutela dei cittadini

A cura di William Nonnis

Un Paese realmente civile, sensibile al benessere della propria cittadinanza, lo si vede dall'attenzione che riserva alla sanità pubblica, dedicando risorse economiche e impegno scientifico al continuo progresso di questo ambito, tanto nevralgico per l'intera società.

Prendersi cura di un paziente significa non solo intervenire direttamente sul suo stato di salute, ma facilitare e semplificare, in ogni modo possibile, il suo rapporto con le strutture sanitarie, offrendo una reale assistenza e supporto a trecentosessanta gradi, proprio nel momento in cui, di fronte ad una malattia, ogni persona si trova in una condizione di fragilità, anche emotiva.

L'innovazione tecnologica, quando non si specchia nelle acque della vanità per dimostrare la propria capacità di oltrepassare "le Colonne d'Ercole", ma si fa concreto sostegno alle attività umane, nell'healthcare può dimostrare tutto il suo valore.

La Blockchain (quella pubblica, cioè permissionless), in particolar modo, con la sua attitudine fortemente sociale e le sue fondamenta ben piantate nella certezza e sicurezza dei dati inscritti nei suoi registri, rappresenta la soluzione digitale alla mancanza di continuità dello storico clinico dei pazienti e di una condivisione di informazioni tra strutture mediche.

Grazie a questa tecnologia, si possono dismettere, infatti, i vecchi faldoni cartacei in cui, finora, si è stati soliti conservare i vari referti medici, a favore di un semplice quanto affidabile click apportando, in tal modo, un cospicuo contributo evolutivo all'archiviazione dei dati.

Perché, consegnare a referti fisici la storia clinica di un paziente, è spesso causa di una consistente discontinuità di informazioni nel percorso sanitario di quel paziente, vuoi per deterioramento dei documenti cartacei, che per il loro smarrimento, creando così un pericoloso vuoto di dati clinici, che può rallentare, se non inficiare, diagnosi tempestive e terapie specifiche, in caso di malattia.

Una chiave digitale, invece, in possesso ad ogni utente del servizio sanitario nazionale, sin dalla nascita, grazie alla Blockchain ha la capacità di divenire un archivio blindato, che restituisce in ogni momento uno specifico dato, oppure tutte le informazioni mediche a disposizione.

I sostanziali benefici di un passaporto sanitario digitale, per il cittadino sono molteplici perché, in tempo reale, oltre a tutto il suo percorso clinico, egli può avere accesso in rete ad iter clinici, che prima richiedevano la presenza fisica dell'assistito nelle aziende ospedaliere di riferimento. Come il cambio del medico di base, ad esempio, che può essere effettuato, in maniera semplice ed istantanea, incrociando i dati di residenza dell'utente, con quelli dei medici presenti nel territorio di pertinenza e, tra quelli, rintracciando i medici con posti disponibili per gli assistiti, rinvenire il medico più adatto alle proprie esigenze.

Facilitare la quotidianità dell'individuo, è il must che l'innovazione tecnologica deve porsi per procurare benessere alla comunità, agevolando anche lungaggini burocratiche, così da restituire un tempo di qualità al cittadino.

Un principio essenziale di facilitazione, che apre a scenari del tutto nuovi, in una realtà in cui, il "buon tempo" di cui siamo sempre in difetto, ci può essere regalato da una tecnologia amica.

E non solo perché, grazie all'utilizzo delle molteplici funzioni integrate nella Blockchain, può tutelare la privacy di accesso ai dati sanitari - argomento molto caro all'ideologia che sottende la Blockchain - è assicurata a tal

punto che quei dati restano di proprietà esclusiva dell'utente, che può sceglierne l'utilizzo.

È nella sua facoltà, infatti, decidere, tra tutto lo storico clinico con il meccanismo della catena di blocchi, composto da anamnesi, referti, cure e terapie, quali informazioni e/o quale branca sanitaria mostrare e a chi, potendo contare su una chiave di accesso differente per ogni referto.

Partendo dall'altro grande beneficio che la Blockchain può procurare in ambito clinico, ossia la condivisione di dati con altre strutture sanitarie - contemporaneamente e in ogni angolo del globo tecnologizzato - un enorme e veloce impulso alla ricerca in campo medico/scientifico è la prerogativa che ne deriva posto che, in tempi pari a zero, il registro distribuito ha la capacità di raccogliere, archiviare, suddividere e incrociare, una quantità infinita di informazioni.

La certezza dei dati inscritti in rete, data l'impossibilità di modificarne o corromperne il contenuto, diviene così una base comune, a livello mondiale, su cui intraprendere nuovi progetti scientifici, avendo a disposizione big data con una mole di informazioni pari a miliardi e miliardi di terabyte.

Con la Blockchain, sensibilissima, come si diceva, nel tutelare la privacy degli utenti, cambia anche l'angolo di visuale della ricerca, perché consente la visibilità e la riconoscibilità, non delle informazioni cliniche, ma dei medici, dei ricercatori e delle aziende che le utilizzano per i propri studi, rendendo i proprietari di quei dati, vale a dire i pazienti, parte attiva e partecipe dei progetti di analisi.

In tempo reale gli esiti scientifici vengono condivisi con il paziente che, a quel punto, con tempi ridottissimi può scegliere dove e come curarsi.

La priorità che la Blockchain assegna alla centralità dell'individuo, la sua libertà, consapevolezza e responsabilità delle proprie scelte, è il fulcro del sistema distribuito che, con l'assoluta circolarità della propria struttura, non solo garantisce un approccio semplificato e affidabile alle informazioni, ma consente un percorso di sviluppo aperto, equo e trasversale delle possibilità.

Inoltre la Blockchain è un elemento importante per la cybersecurity, un contributo alla sicurezza ma non una soluzione.

Un'"umanizzazione" delle cure, verrebbe da dire, da parte di questa tecnologia, che sostiene una nuova humanitas e che, proprio nel settore dell'healthcare, apre al meglio il suo ventaglio di opportunità e utilità sociale.

"La Blockchain è un elemento importante per la cybersecurity, un contributo alla sicurezza ma non una soluzione".

NIS-2 perché è importante conoscerla!

A cura di Davide Giribaldi

Quarantasei articoli, tre allegati, centoquarantaquattro considerando.

È questa l'estrema sintesi della nuova Direttiva NIS-2 (Dir. UE 2022/2555) che stabilisce misure volte a garantire un livello comune elevato di #cybersecurity nell'Unione Europea per migliorare il funzionamento del mercato interno.

Ha tre obiettivi:

1. Aumentare il livello di resilienza informatica di tutti i soggetti pubblici e privati che rientrano in perimetro.
2. Ridurre le incoerenze nei settori già coperti dalla direttiva attuale.
3. Migliorare il livello di consapevolezza comune e la capacità collettiva di preparazione e risposta agli incidenti.

È parte di un pacchetto più ampio di misure strategiche a livello europeo a tutela dei principali aspetti che regolano la sicurezza delle informazioni a livello complessivo e che comprende tra gli altri il GDPR, il Cybersecurity Act, il Regolamento DORA per la gestione dei rischi informatici degli operatori del mercato finanziario e la Direttiva CER sulla resilienza delle Infrastrutture critiche.

È applicata a tutte le entità pubbliche e private di "medie dimensioni" che rientrino negli undici settori di mercato definiti ad "alta criticità" e nei sette considerati come "critici".

Per comprendere l'estensione dei soggetti a cui la Direttiva è rivolta, è opportuno chiarire che le "medie dimensioni" sono quelle definite dall'art.2 par.1 dell'allegato alla Raccomandazione 2003/361/CE, ovvero tutte le organizzazioni private con meno di 250 dipendenti, fatturato annuo non superiore ai 50 milioni di Euro, bilancio annuo non superiore ai 43 milioni di Euro.

La NIS-2 inoltre, distingue tra operatori di servizi "essenziali" e "importanti".

Tra i primi sono ricomprese le Pubbliche Amministrazioni, e le aziende dei settori energetico, delle infrastrutture digitali, sanitario, bancario, dei trasporti e delle acque.

Tra gli operatori di servizi "importanti" ci sono quelli legati ai servizi postali e i corrieri, quelli relativi alla gestione dei rifiuti, al settore chimico, agroalimentare e produttivo in genere.

Prima di pensare che la vostra organizzazione si collochi al di fuori del perimetro di applicazione della Direttiva, è bene sapere che la NIS 2 pone una forte attenzione alla cosiddetta supply chain, prevedendo il monitoraggio della sicurezza della catena dei fornitori.

Per questo motivo è probabile, che nel caso vi troviate ad operare per aziende pubbliche o private che rientrino in uno di questi settori, i vostri clienti possano richiedervi il rispetto di requisiti minimi di sicurezza, piuttosto che sottoporre la vostra organizzazione ad audit di conformità normativa.

Nel caso non lo foste già, potrete farvi trovare pronti adottando un framework che vi consenta di realizzare (anche senza certificarlo formalmente) un sistema di gestione per la sicurezza delle informazioni.

Qualche esempio?

Il più semplice in assoluto è il Framework per la Cybersecurity Nazionale, che offre un set minimo di controlli a cui adeguarsi, senza necessariamente sconvolgere le procedure aziendali.

Se invece cercate qualcosa di più strutturato, potete guardare la versione 8 dei Controlli CIS, piuttosto che il Framework NIST sulla cybersecurity. Al di sopra di tutto c'è poi la possibilità di adottare un sistema di gestione in conformità alla norma ISO/IEC 27001:2022 che rappresenta il più ampio elemento di garanzia tanto per voi quanto per i vostri clienti.

La novità più importante introdotta dalla NIS-2 è l'obbligo di segnalazione degli incidenti da parte di entrambe le categorie di operatori (essenziali e importanti) che senza indugio e comunque nel termine massimo di 72 ore (GDPR docet!) dalla venuta a conoscenza di una violazione, dovranno procedere alla notifica ai CSIRT designati dagli Stati Membri, che dovranno agire da intermediari fidati e dovranno facilitare l'interazione tra i soggetti segnalanti e i produttori/fornitori di prodotti e servizi TLC, sotto l'egida di ENISA, l'Agenzia Europea per la Cybersecurity che dovrà creare e mantenere un registro europeo delle vulnerabilità individuate.

A tale proposito la Direttiva dedica un intero Capo di sei capitoli (20-25) alle misure di gestione del rischio cybersecurity e ai relativi obblighi di segnalazione.

Lo fa ad altissimo livello, introducendo con chiarezza le misure "minime" che chiunque ricada nel perimetro deve adottare con un approccio multirischio.

Tra queste, oltre alla già citata sicurezza della catena di approvvigionamento (che dovrà comprendere tutti gli aspetti di cybersecurity riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi), ci sono le politiche di analisi dei rischi e di sicurezza dei sistemi informatici, la continuità operativa e la gestione delle crisi.

La Direttiva NIS-2 dovrà essere accompagnata da norme di recepimento a livello nazionale e sarà operativa a partire dal 17 ottobre 2024.

Un lasso di tempo relativamente breve, per comprendere a fondo la trasformazione a cui dovremmo sottoporre le nostre aziende. Un tempo comunque sufficiente per formare ed informare tutto il personale coinvolto, per fare le opportune valutazioni e perché no, predisporre piani di mitigazione dei rischi e di risposta agli incidenti, sui quali almeno in linea teorica, dovremmo essere già tutti preparati.

La NIS-2, distingue tra operatori di servizi "essenziali" e "importanti".

Cyber-Crimine: i sussurri che cambieranno la sicurezza delle nostre Aziende

A cura di Luca Mella

Introduzione

Sappiamo benissimo che nel corso dell'ultimo anno il panorama della sicurezza cibernetica è cambiato in maniera sostanziale: il conflitto russo-ucraino ha incendiato molti animi, specie nel mondo digitale. Nel corso del 2022 si sono infatti susseguite notizie di nuovi attacchi, nuove campagne, attacchi dimostrativi e, non da meno, fiumi di propaganda bipartisan che hanno esondato su social e piattaforme.

Questo è quanto tutti abbiamo notato, ed è quanto tutti ci hanno fatto notare. Tuttavia, l'intento di questo articolo è soffermarsi su alcuni dettagli, alcune ripiegature delle vicende che tutti abbiamo udito dal 24 Febbraio 2022 di anno scorso ad oggi e che, probabilmente, abbiamo colto solo in parte. Difatti, come esperti del settore digitale, ma anche come esperti nel settore della sicurezza, qualcosa abbiamo perduto nella baraonda mediatica che si è susseguita dall'inizio del conflitto.

Gli aspetti più interessanti, almeno agli occhi dell'autore di questo articolo, si celano tra le connessioni di quello che già conosciamo del mondo del cyber crimine e gli spiragli che le tensioni geopolitiche hanno aperto nel sottobosco digitale. Spiragli dai quali è filtrata abbastanza luce da permetterci di individuare tendenze in atto, altrimenti passate in sordina.

Dobbiamo preoccuparcene?

Il primo, e più a noi prossimo tema a cui va prestata particolare attenzione, è il mondo della ricerca di vulnerabilità. Nel settore della sicurezza, da tempo siamo abituati ad avere a che fare con ricercatori che pubblicano articoli su vulnerabilità software, questioni etiche sulla divulgazione delle falle e dibattiti infiniti sui modi migliori di trattare questi rilievi così critici per chi produce e chi usa il software. Molto meno spesso siamo invece abituati ad interrogarci sul come chi compie atti criminali ragioni ed operi su questo stesso tema.

Il Passato

Prima di puntare lo sguardo verso la luce trapelata grazie alle schermaglie digitali, occorre riprendere quanto già sappiamo sulle attività di ricerca di vulnerabilità nel sottobosco digitale: è infatti risaputo che i gruppi APT che operano all'interno degli ecosistemi state-sponsored conducano programmi di ricerca di nuove vulnerabilità ed abbiano capacità di sviluppo di vulnerabilità 0-day, falle di sicurezza note solo a loro e non ai produttori del software.

Questa consapevolezza fonda le sue radici decenni addietro ed ha senz'altro raggiunto le masse a partire dal caso Stuxnet, nel lontano 2010, quando i servizi di intelligence statunitensi ed israeliani codificarono ben quattro exploit per vulnerabilità 0-day all'interno del loro impianto malware. A partire da quel momento, negli anni, è stato un susseguirsi di notizie di 0-day sfruttati da attori state sponsored cinesi, russi o iraniani, una volta per Internet Explorer, poi per Adobe Reader, poi ancora per WhatsApp, per iOS, per Microsoft Exchange Server, e così via.

Non solo. Negli ultimi dieci anni si sono uniti a questa compagnia anche agenzie private come la defunta HackingTeam e l'israeliana NSO Group, autrice dell'impianto Pegasus e di diversi 0-day per sistemi iOS. Questi sono gli attori che storicamente praticano ricerca di vulnerabilità nel panorama delle minacce cibernetiche tradizionali.

Nuovi Player

Ed il crimine cibernetico? Il cyber-crimine è molto spesso stato allontanato dal tavolo degli adulti quando si trattava di 0-day. Questo perchè tradizionalmente gli attori criminali utilizzano i cosiddetti exploit 1-day, ovvero codici in grado di sfruttare falle già note ai produttori di software: in altri termini, codici per sfruttare quelle CVE in cui chiunque abbia mai lanciato una scansione di vulnerabilità si è ineluttabilmente imbattuto.

Il punto è che sempre più attori criminali sono diventati molto bravi nello sfruttare attacchi 1-day, e sempre più veloci nel farlo. Un dato per tutti è quello di ProxyLogon, la falla che nel 2021, tre giorni dopo la pubblicazione della sua patch, è stata presa d'assalto da una pletora di attori criminali che l'hanno usata per migliaia di organizzazioni in tutto il mondo. Il tutto in pochissime ore.

La voracità degli attori cyber criminali non è affatto calata: se spesso li classificavamo come attori di secondo piano, una sorta di Tier-B. Tuttavia, oggi dobbiamo ricrederci, o almeno riconsiderare le capacità e la pericolosità di questo segmento di minacce.

Ciò che è accaduto in tema 0-day nel mondo cyber criminale è esemplare: nell'ultimo anno, anche gli ambienti cyber criminali hanno dimostrato di saper attingere alle falle 0-day. Ne abbiamo avuto l'esempio anche recentemente nell'Aprile 2023, quando Microsoft stessa ha rilasciato patch per una falla 0-day, la CVE-2023-28252: una particolare vulnerabilità all'interno del driver di sistema "clfs.sys", utilizzato dai sistemi operativi Windows per la gestione di servizi di logging per applicazioni e componenti.

In base alle ricostruzione del GReAT di Kaspersky, questa falla è stata utilizzata da un particolare attore ransomware Nokoyawa durante intrusioni ed estorsioni in ambienti Retail, Manifatturiero, e Sanitario. Verticali ben diversi dai soliti a cui siamo abituati a immaginare quando pensiamo alla minaccia degli 0-day.

Al di là dei verticali impattati, l'elemento forte è l'attribuzione dello sfruttamento di questi particolari 0-day ad un attore puramente criminale: un gang che opera attacchi ransomware secondo il modello delle "double extortion", pratica estorsiva cyber criminale che vuole accostata all'attacco ransomware una serie di pratiche estorsive secondarie, a partire dal furto massivo di dati riservati e la relativa minaccia di pubblica diffusione.

Sussurri (poco) lontani

Avevamo avvisaglie di questa evoluzione? La risposta è sì. E come anticipato molto più di qualche elemento trapelò proprio a valle delle "operazioni speciali" del regime russo in Ucraina. Di fatti, pochi giorni dopo all'inizio dell'invasione, l'underground digitale criminale fu profondamente scosso da prese di posizione bipolari: ci fu chi si astenne da qualsiasi fazione, come LockBit, e chi come Vice Society e Conti dichiararono pieno supporto alla causa russa. Una delle conseguenza di questi atteggiamenti fu il "Conti Leak".

Il Conti Leak è stata una delle fughe di dati più significative che ha coinvolto gli ambienti cyber criminali. Dopo la presa di posizione della gang Conti a supporto della causa russa, alcune gole profonde di diversa opinione hanno affondato il colpo: anni di conversazioni interne della gang e codici sorgenti sono stati pubblicati sul web rivelando molti dettagli di estremo interesse per le Threat Intelligence di tutto il mondo.

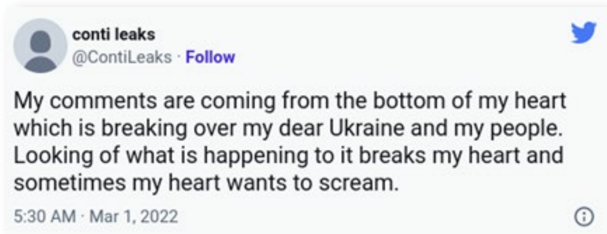


Figura. Annuncio pubblicato da "Conti Leak" nel Marzo 2022

Oltre alla conferma dei sospetti delle influenze governative all'interno dei gruppi criminali maggiori, una sorta di regia occulta che orienta alcune delle campagne criminali e che richiederebbe un approfondimento dedicato, alcuni dettagli emersi in questi file completano particolarmente bene quanto abbiamo cominciando ad osservare recentemente con i casi di gang come Nokowaya, che, appunto, ha sviluppato 0-day indipendentemente.

Dai Conti Leaks abbiamo modo di trovare traccia di alcuni apparentemente lontani sussurri che presagivano che questo momento sarebbe ad un certo punto divenuto reale: il cyber crimine sta infatti progredendo molto in fretta nello sviluppo di capacità di ricerca di vulnerabilità e implementazione di pericolosissimi 0-day.

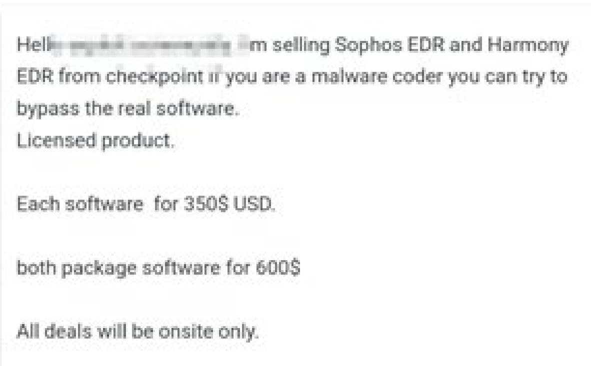
Conti ha da precursore in questo ambito e l'orientamento fornitogli dai servizi segreti russi ha senz'altro giocato un ruolo nei risultati ottenuti da questa pericolosa gang. Conti, infatti, approciava l'attacco esattamente come fanno le compagnie di spionaggio:

- Conduceva ricerca di vulnerabilità interna per 0-day, ad esempio per router e firewall Cisco.
- Sviluppava scanner di vulnerabilità ed exploit personalizzate per falle 1-day, come ad esempio nel caso della CVE-2020-5135 di SonicWall.
- Si approvvigionava di exploit 0-day da terze parti nel mercato nero.

Approcci che a distanza di un anno sono state riscontrate anche su altre gang criminali che praticano le doppie estorsioni, proprio come nel caso appena menzionato di Nokoyawa: gruppo ransomware operativo solamente da Aprile 2022 e che nel giro di pochi mesi ha sviluppato proprio queste capacità di accesso a vettori 0-day.

Altro elemento precursore che ci arrivò agli inizi della guerra fu nella direzione della sofisticazione nella capacità di evadere le difese a protezione delle aziende. Sempre all'interno del Conti Leak, alcune delle conversazioni dei criminali riportavano infatti di una serie di società di facciata utilizzate dai criminali per acquisire licenze e software di difesa. Ad esempio, licenze del sistema di protezione endpoint di nuova generazione Carbon Black, prodotto da VMWare, acquistate dalla gang ai fini di "ricerca interna". Ricerca che all'atto pratico significa identificazione di metodi di bypass ed evasione dei moderni strumenti di protezione.

Anche questo elemento ha disegnato una preoccupante traiettoria nel mondo cyber criminale. A Marzo 2023 è stata infatti tracciata all'interno dei mercati criminali una serie di vendite illecite di prodotti di sicurezza: Sophos EDR, Harmony EDR, Crowdstrike XDR, e Palo Alto Cortex XDR, ed ancora Carbon Black (link). Una serie di tecnologie di fascia altissima, riconosciute a livello mondiale e ben più ricca di quella molto più ricca emersa dalle conversazioni trafugate da Conti un anno prima.



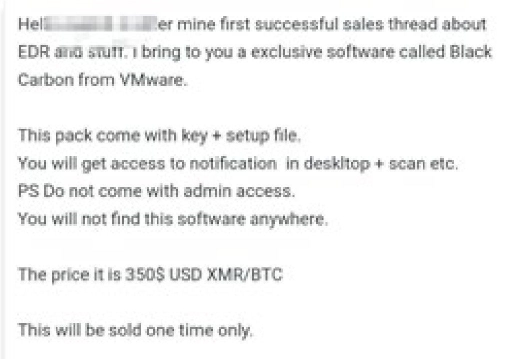


Figura. Estratto dagli annunci di vendita illeciti nei mercati criminali

Dove ci stiamo muovendo?

A distanza di un anno, le pratiche della ex-prima gang cyber criminale russa si sono diffuse ad altri attori del crimine cibernetico: il fenomeno è impressionante specie per le tempistiche più brevi delle attese. Tuttavia, il dato della velocità non è l'unico elemento preoccupante: la sofisticazione delle minacce cyber criminali è ormai da considerarsi una direzione assodata, persino per le minacce che un tempo classificavamo come "di serie B": ora in procinto di essere pericolose quasi quanto le più blasonate.

Questo movimento nell'underground criminale rappresenta una cambio epocale nei profili di minaccia che siamo abituati a trattare, specie nelle fasce di aziende medie ed in tutte le grandi al di fuori dei settori tradizionalmente interessati dalle minacce state sponsored. Occorre aumentare drasticamente i livelli di difesa perché, come abbiamo osservato, il crimine cibernetico sta rapidamente raggiungendo livelli di minaccia comparabili ad attori molto strutturati, attori che tradizionalmente non prendevano di mira queste tipologie di aziende: ora, questi segmenti di business cominciano a ricevere attacchi ad un livello precedentemente inaudito nella loro storia.

Lo spirito del terrorismo: un'analisi sociale

A cura di Marco Santarelli

Lei parla spesso di Terrorismo sociale, cosa intende?

Proviamo a mettere un punto alla disinformazione: la parola terrorismo, etimologicamente affibbiata alla parola francese *terrorism*, in realtà deriva da *terròrem*, dal verbo latino *terreo*, che significa spaventare, derivante a sua volta da *ex-pavèntare*, esteso al participio presente *ex-pàvens*. Simultaneamente spaventare e paventare, cioè trasmettere paura attraverso un evento e far percepire e ingigantire quello che si propaga nella società e nella popolazione, che fanno a loro volta da cassa di risonanza. Questo vuol dire che nessuno di noi è più al sicuro. È in gioco la nostra quotidianità. Siamo possibili bersagli, destinatari di eventi terroristici diretti ai servizi essenziali per noi. Le cosiddette Infrastrutture Critiche, infatti, possono essere attaccate provocando interruzioni di linee di sopravvivenza (cibo, acqua, energia e così via). Anche se non attaccati direttamente su beni primari e sostanziali, possiamo venire attaccati attraverso il nostro tessuto sociale, decisionale e informativo, come avviene per le fake news e l'indirizzamento delle decisioni. È terrorismo anche questo, cioè parte da questo concetto di terrorismo, come abbiamo visto. Quindi sociale perché riguarda tutti noi.

Come spiegato in "Sociological analysis of new terrorism between dynamics of radicalization and programs of de-radicalization"[20] (Analisi sociologica del nuovo terrorismo tra dinamiche di radicalizzazione e programmi di de-radicalizzazione) di Patrizia Laurano e Giuseppe Anzera, già negli anni '40 si è iniziato a parlare di Social Movement Theory, o SMT, ossia di evoluzione della minaccia terroristica, che permea nel tessuto sociale. Si pensava che i movimenti emergessero da processi e comportamenti irrazionali che si registravano in condizioni ambientali che portavano malcontento. Da qui, dalla sottomissione passiva a forze sociali travolgenti, l'adesione degli individui al movimento. Negli anni '80 e '90 ci si è accorti di un aspetto più razionale dietro ai processi e il movimento doveva sopravvivere. Per farlo, era necessario creare un corpo di supporter per sostituire le perdite e diffondere la sua influenza. I soggetti seguivano un iter di reclutamento incentivante e attento alla selezione dei più adatti per persuadere le reclute ad aderire, aspetti che necessariamente trovano maggiore forza nei legami sociali e nelle relazioni. Alla fine del secolo scorso, sono nate due nuove tendenze all'interno della SMT, ossia la New Social Movement Theory, incentrata sui processi macro-strutturali, e la Resource Mobilization Theory, attenta ai processi contestuali come le dinamiche di gruppo. Una terza tendenza, individuata da Anja Dalgaard-Nielsen del Danish Institute for International Studies, è chiamata Framing Theory, che si concentra sulle narrazioni e i significati che vengono prodotti dai movimenti e dalle collettività sociali. Il movimento punta alla diffusione di un messaggio che sia più aderente possibile a interessi, atteggiamenti e credenze dei soggetti, portandoli a vedere la realtà così come la vede il movimento stesso. Questo aspetto è stato chiamato *frame alignment* e, secondo Dalgaard-Nielsen, l'approccio della Social Movement Theory, ma soprattutto della Framing Theory, può favorire la comprensione della radicalizzazione, dato che il focus è sui processi e non solo sui dati, con un'analisi di livello intermedio tra macro e micro. In tale contesto si sviluppano delle cellule che a loro volta producono delle reti, che chiamerei informative, che minano, quindi, ogni tipo di assetto di pace di ogni Stato democratico. Questo fa tramontare l'idea, soprattutto dopo il 2001 [attacco alle Torri Gemelle, ndr] e dopo gli attentati a Parigi, Madrid e Berlino, che viviamo in una pace perenne o di base, in cui i cosiddetti stati di necessità o di emergenza sono momenti eccezionali. Al contrario, è giusto pensare che le misure straordinarie non siano più riconducibili al terrorismo, ma alle crisi climatiche (tra cui terremoti e tsunami, ad esempio), pandemiche o, in generale, estranee alle questioni umane. Nell'ordinamento di una società il terrorismo è collegato ai poteri ordinari e a quelli speciali, non a cause astruse o più grandi di noi. Quindi, la domanda principale non deve essere cosa facciamo, ma come lo facciamo, evidenziando limiti procedurali e sostanziali di provvedimenti d'emergenza finora risultati troppo poco conformi alle persone stesse. Come sostiene Domenico Tosini nell'articolo "Sociologia dell'antiterrorismo: la struttura della lotta al terrorismo nelle democrazie liberali" [21], il terrorismo evidenzia la perdita di controllo dello Stato e, di conseguenza, l'incapacità di proteggere i cittadini. Il terrorismo, in questo modo, "erode la fiducia dei cittadini nell'efficienza del proprio stato, così privandolo di una delle fonti più importanti della legittimità dell'uso della forza fisica – e, quindi, della legittimità della sua sovranità (com'è noto da Hobbes in poi)"[22]. In sostanza, per le persone è un rischio alla propria sicurezza, per lo Stato una minaccia alla sovranità.

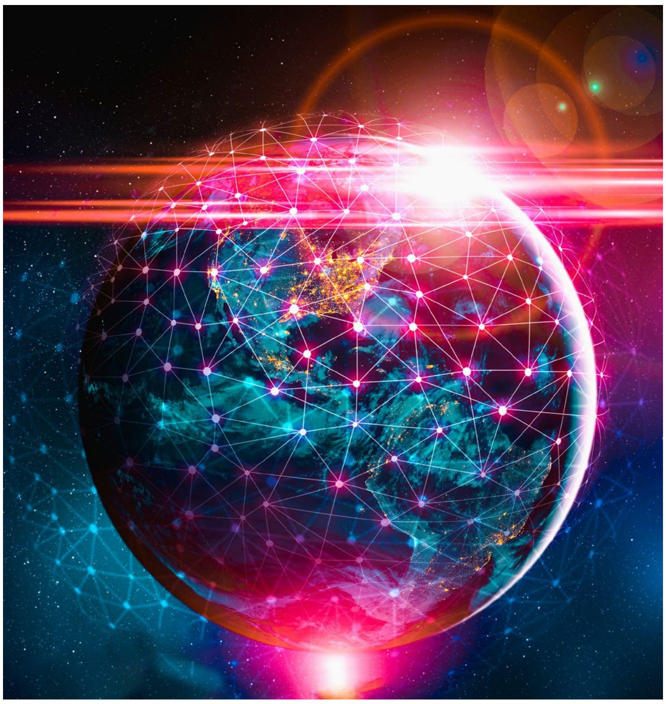
Come nascono le reti nel Terrorismo sociale e come si sviluppano fino a farlo diventare organizzato?

Il terrorismo si espande, secondo un punto di vista contemporaneo, come struttura e configurazione di reti organizzate. Le reti si sviluppano e si ritraggono come un elastico, dando più o meno valore aggiunto. In questo scenario lo sviluppo è nella costituzione di reti compiacenti che fanno sì che il terrorismo sia sociale perché alimentato soprattutto dal suo interno e, trasversalmente, da altre reti criminali. Crea l'illusione di una vita migliore, amplifica disagi, cresce, fa studiare, trascina con sé soggetti problematici che vogliono dare ai figli speranze che, invece, si rivelano solo delle illusioni. Cresciute queste reti (come coordinate o, raramente, cani sciolti) sviluppano la loro dialettica in un classico trittico: si individua qualcuno a cui raccontare ciò che si vuole fare (crescita del disagio e sviluppo di dipendenze tra persone), si sceglie un destinatario (un potere da combattere o un luogo) e si costruisce la strategia sul messaggio come narrazione (racconto, analisi premeditata di chi svolge l'attentato, cosa rappresenta e come si deve muovere tra studi approfonditi dello stesso attentato, spaventare). Il terrorismo, così facendo, diventa organizzato e, come tale, si amplia per esplorare l'infinità di forme di un'azione da intraprendere.

Vediamo qualche esempio che ci fa capire meglio come agisce il Terrorismo sociale.

Gli attentati del dopoguerra, dell'omicidio Moro, la facilità di gestire fondi per attentati della criminalità organizzata (con conseguente aumento della percezione del benessere verso quelle persone che non hanno possibilità di credito immediato) in Italia e l'attentato ai mercatini di Berlino del 2016 ne sono la stessa medaglia con facce diverse. La fotografia perfetta del terrorismo. Nel primo caso, quello degli attentati del dopoguerra, si lancia il messaggio simbolico della morte per sacrificare la stessa idea di democrazia con una precisa connotazione di potenza latente e mostruosa. Questo è un terrorismo ancora attivo che intende far emergere la compiacenza, come si nota in un documento molto interessante del

1992 del Senato della Repubblica[23], tra professionisti, politici e terroristi. Un terrorismo che, appunto, abbiamo definito sociale. Ingranaggio stesso del tessuto sociale. Striscia, penetra e agisce grazie a soggetti insospettabili. Per il caso dell'attentato di Berlino del 2016, simile a quello di Nizza, Parigi o Vienna, i terroristi hanno approfittato delle variabili e delle connessioni che si sono costituite tra organizzazione perfetta, coincidenze e implicazioni, proponendo un'angolatura legata, questa volta, a una mondializzazione del concetto stesso di terrorismo. Infatti, dalle Torri Gemelle in poi, si assiste a questo tipo di terrorismo globale, appunto. Non è più solo sociale, ma si estende a un messaggio più alto. Ecco che, per Berlino, l'attacco è avvenuto intorno alle ore 20:15. Qui il tessuto sociale individuato non è lo scopo, ma il mezzo. L'atto è stato studiato proprio per questo: è avvenuto a Breitscheidplatz, nei pressi della Kurfuerstendamm, vicino alla chiesa intitolata al Kaiser Guglielmo, ovvero allo stesso tempo luogo centrale e obiettivo primario nella zona più commerciale della parte occidentale della città e molto frequentata, oltre che da residenti, anche da turisti. Questi ultimi erano il vero obiettivo. Questo tipo di terrorismo tende a voler trasmettere il messaggio non solo alle persone del luogo, ma al mondo intero. Il messaggio era ed è anche quello di avvertire altri Paesi. A questi possiamo abbinare, con tecniche diverse, quegli attentati che avvengono in luoghi pubblici, aeroporti, ambasciate (vedi quello dell'italiano Attanasio) e così via. Di solito la rivendicazione è l'atto finale che tende a destabilizzare l'idea stessa di democrazia mondiale. Ma non solo: si mira a trasformare il mondo attraverso il concetto di sacrificio che si realizza con la forza. Il punto cruciale, partito dalla civiltà illuministica e rinascimentale, è che nessuno ha mai ben capito che il Bene, il progresso, la tecnologia e l'innovazione crescono insieme al Male, ovvero insieme a chi li utilizza anche per altro. Si innesca una tattica che possiamo chiamare eccesso di realtà, os-



sia uno specchio della realtà stessa, come dice il filosofo Jean Baudrillard. Secondo quest'ultimo, il terrorismo è molto simile alla terapia del caos o della complessità. Uno choc iniziale provoca conseguenze notevolmente più ampie rispetto all'evento grazie all'evento stesso e alla comunicazione che si crea intorno a esso. Basta riprendere, appunto, il già citato attacco delle Torri Gemelle del 2001. Gli eventi stessi sono stati parte del gioco, nel loro manifestarsi, perfezionando l'evento come trauma simbolico.

Trauma simbolico significa anche conoscere meglio i fenomeni?

Il trauma simbolico fa partire l'ultimo atto che chiude la dialettica dei tre momenti, di cui sopra: la narrazione. Narrare è conoscere. Come ci ricorda l'etimologia stessa di narrazione. Ovvero, anche osservare per tanto tempo, infiltrarsi nella vita quotidiana, abbassare le difese percettive, attivare una rete di informatori, capire, destrutturare le informazioni e creare un piano preciso. Il legame tra terrorismo, narrare e conoscere è stretto. Narrare da gnarigàre, (purgare, ripulire, essere esperto di, conoscitore) e narro (racconto), i quali trovano a loro volta corrispondenze nella lingua greca (verbo gignosko, conosco). Entrambe rimandano a una radice sanscrita (gnâ), conoscere. Narrare come raccontare, che richiama la coppia legein-logos del greco antico. Narrare significa anche deformare, deturpare e violare le leggi costituite attraverso mezzi e civili inermi. La percezione della realtà con la narrazione viene molto amplificata, si generano una visuale e un'angolatura che servono prevalentemente a chi prepara l'attentato per imporre il proprio potere, barattare le proprie richieste e, soprattutto, avere gli strumenti per capire come prepararne altri e come gestire le criticità di quelli già organizzati. La minaccia terroristica attraverso la narrazione, il racconto, fa passare il terrorismo da globale (tendenzialmente attivo fino al 2016) a quello della porta accanto di oggi, generando psicologicamente il cosiddetto adattamento e assuefazione alla minaccia. Non c'è un terrorismo afghano o siriano, ce ne sono tanti che sfuggono all'opinione pubblica, ma che strisciano sempre più organizzati, coerenti (ahinoi) e che dialogano senza sosta.

In merito alla molteplicità del campo di battaglia, ha senso parlare di Terrorismo sociale?

Il terrorismo tendenzialmente si manifesta con armi nucleari, biologiche, chimiche, radiologiche, droni, automazione della IoT, sviluppo di stampanti 3D, social, psicologia, spazio, armi fisiche e così via. Il nemico è trasversale, supera la nazione di appartenenza. Il terrorismo è, però, da sempre, strategia, come detto, mondializzazione dei messaggi, al di là, che sia chiaro una volta per tutte, degli strumenti normativi o innovativi che, invece, vengono sfruttati in base al cambiamento della società. I due fenomeni non si muovono in modo sincronico. Non esiste un terrorismo degli strumenti, di cui si sta parlando sempre più, ma esiste un terrorismo endemico che ha alla base una rete, come detto, che attraversa una sua organizzazione perfetta, che porta solo dopo alla scelta degli strumenti che vengono utilizzati, mai il contrario. Come arginiamo questo fenomeno? Esistono tanti documenti e studi in merito. Uno molto importante è quello del 29 settembre 2021, redatto dal Parlamento Europeo, che si sviluppa su quattro assi per una migliore risposta condivisa: il primo è sui controlli di sicurezza per prevenire le infiltrazioni; il secondo è sullo sviluppo di una visione strategica da parte dell'Intelligence; il terzo è sul monitoraggio e sul contrasto della propaganda con la mobilitazione dello sviluppo e coordinamento di reti informative locali e non; il quarto consiste nell'affrontare la criminalità organizzata come fonte trasversale di finanziamento del terrorismo.

La convergenza della cybersecurity: un ruolo chiave per le organizzazioni

A cura di Petra Chistè

In un'epoca in cui la digitalizzazione e l'interconnessione hanno rivoluzionato il mondo degli affari, la convergenza della sicurezza emerge come una tendenza fondamentale nel settore ICT.

La convergenza della sicurezza rappresenta l'integrazione delle strategie e delle tecnologie di sicurezza informatica, sicurezza fisica e gestione dei rischi, per una protezione più completa e armonizzata delle risorse aziendali.

In questo articolo, esploreremo come la convergenza della sicurezza può essere implementata nelle organizzazioni, affrontando le sfide e svelando i vantaggi di questa strategia, indispensabile per garantire la resilienza e il successo delle imprese moderne.

Nella cronaca recente siamo abituati a vedere aziende colpite da ransomware o grandi incidenti fisici con lo scopo di rubare i beni aziendali, vedi gli attacchi agli ATM.

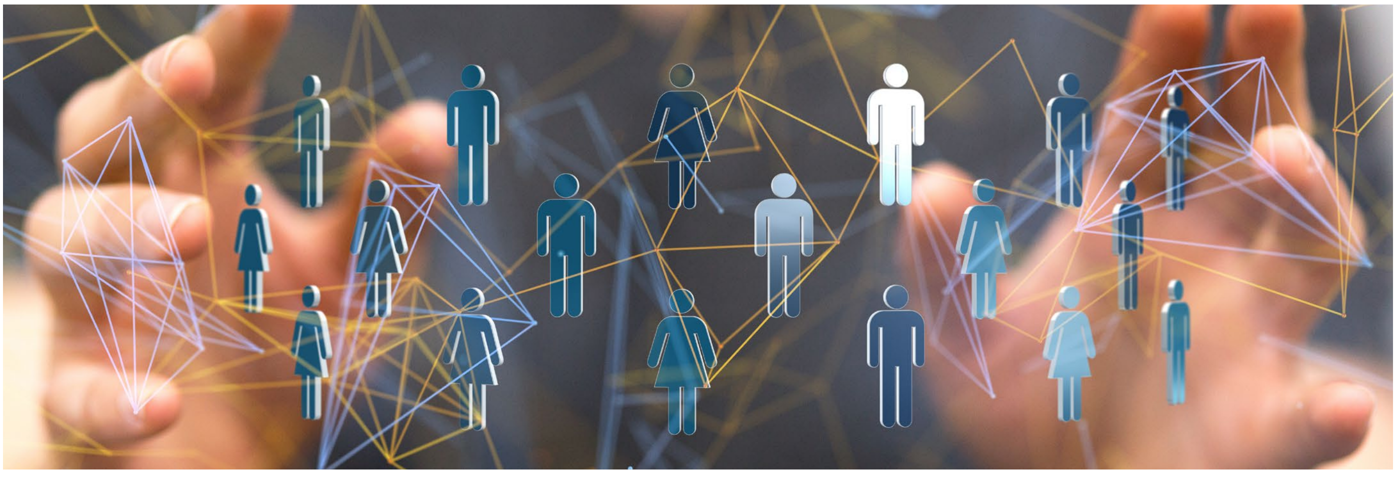
Ma la narrazione ci racconta anche di casi dove la commistione dei due tipi di attacchi ha portato ad una grave minaccia per la sicurezza delle persone.

Un esempio di un incidente di sicurezza informatica che ha avuto ripercussioni sulla sicurezza fisica riguarda un impianto di trattamento delle acque in Israele[24]. Nel 2020, un attacco informatico ha preso di mira gli impianti di trattamento delle acque del paese, cercando di modificare i livelli di cloro nell'acqua. Gli aggressori hanno sfruttato una vulnerabilità in un sistema SCADA (Supervisory Control and Data Acquisition) per accedere ai controlli degli impianti. Sebbene l'attacco sia stato rilevato e neutralizzato prima che potesse causare danni, se fosse stato portato a termine con successo, avrebbe potuto avere gravi conseguenze sulla sicurezza fisica, come il rischio di avvelenamento dell'acqua potabile per migliaia di persone.

Un esempio di un attacco che ha sfruttato invece la sicurezza fisica per accedere a sistemi informatici critici è l'operazione "Stuxnet"[25]. Stuxnet è un worm informatico scoperto nel 2010, che ha attaccato i sistemi di controllo industriale, in particolare quelli utilizzati nei programmi nucleari iraniani. L'attacco ha avuto inizio quando gli aggressori hanno introdotto il worm Stuxnet in un impianto nucleare iraniano tramite una chiavetta USB, sfruttando una falla nella sicurezza fisica. Una volta all'interno del sistema, Stuxnet ha preso di mira i sistemi di controllo dei centrifugatori utilizzati per arricchire l'uranio, causando malfunzionamenti e ritardi significativi nel programma nucleare iraniano. L'operazione Stuxnet è un esempio di come la compromissione della sicurezza fisica possa portare a gravi conseguenze per i sistemi informatici critici e per le infrastrutture di un paese.

In tale contesto, caratterizzato da crescenti rischi cyber e minacce fisiche, la convergenza della sicurezza assume un ruolo cruciale per garantire la continuità operativa delle imprese. Il suo obiettivo principale è quello di creare un ambiente sicuro e resiliente, in cui le diverse funzioni di sicurezza collaborino sinergicamente per affrontare le sfide e le vulnerabilità emergenti.

Ma come si può implementare la convergenza della sicurezza in un'azienda per sfruttarne appieno i benefici?



Per implementare con successo la convergenza della sicurezza in un'azienda, è fondamentale adottare un approccio graduale e strutturato. Alcuni passi ne permettono una adozione efficace.

La valutazione delle esigenze è un passo fondamentale nel processo di convergenza della sicurezza. È essenziale identificare le aree critiche e le vulnerabilità dell'organizzazione, analizzando sia gli aspetti fisici che quelli informatici. Questo permette di avere un quadro completo dei rischi e delle necessità di protezione, permettendo di elaborare una strategia di sicurezza adeguata e mirata.

Una volta comprese le esigenze, è importante creare un team multidisciplinare che coinvolga esperti di sicurezza informatica, sicurezza fisica e gestione dei rischi. Lavorando insieme, questi professionisti possono elaborare una strategia integrata che tenga conto di tutte le sfaccettature della sicurezza e delle possibili minacce. Il coinvolgimento di diverse competenze e prospettive è fondamentale per garantire un approccio olistico e completo alla protezione dell'organizzazione.

La formazione e la consapevolezza del personale su temi di sicurezza è un altro elemento chiave nella convergenza della sicurezza. È essenziale sensibilizzare e formare i dipendenti su questi argomenti, promuovendo una cultura di responsabilità condivisa all'interno dell'azienda. Ciò contribuirà a garantire che tutti i membri dell'organizzazione comprendano l'importanza della sicurezza e siano pronti a identificare e segnalare eventuali minacce.

Infine, è cruciale implementare un sistema di monitoraggio e valutazione continua delle minacce per aggiornare e migliorare costantemente la strategia di sicurezza. Attraverso un'analisi costante delle minacce emergenti e delle vulnerabilità interne, l'organizzazione può adattare la sua strategia di sicurezza per far fronte alle nuove sfide e assicurare una protezione efficace e resiliente nel tempo.

Tuttavia, nonostante i numerosi vantaggi, implementare la convergenza della sicurezza non è privo di sfide. Quali sono le principali difficoltà che le aziende devono affrontare in questo processo?

La resistenza al cambiamento può essere un ostacolo significativo quando si cerca di implementare la convergenza della sicurezza nelle organizzazioni. In particolare, i dipendenti che lavorano nei settori della sicurezza fisica e informatica potrebbero essere riluttanti ad abbracciare nuovi approcci e metodi. Per superare questa resistenza, diventa fondamentale promuovere una cultura aziendale aperta al cambiamento, garantendo una comunicazione chiara e trasparente sui benefici della convergenza della sicurezza.

Uno degli aspetti cruciali della convergenza della sicurezza è la necessità di nuove competenze e conoscenze per i team coinvolti. Per affrontare con successo le sfide emergenti nel panorama delle minacce, è vitale fornire formazione adeguata e aggiornata ai dipendenti, assicurando che siano pronti a gestire queste nuove sfide.

Nel contesto della convergenza della sicurezza, anche la gestione delle politiche interne diventa fondamentale. Le organizzazioni potrebbero dover ripensare le politiche e le procedure interne per garantire che le diverse aree di sicurezza lavorino insieme in modo efficace. Ciò potrebbe includere la creazione di nuovi ruoli, come il responsabile della sicurezza convergente, che supervisiona sia la sicurezza fisica che quella informatica.

Un altro ostacolo potrebbe riguardare l'interoperabilità e l'integrazione dei sistemi di sicurezza fisica e informatica. Spesso, questi sistemi sono progettati e gestiti separatamente, creando sfide tecniche per le aziende che cercano di integrarli. Per superare questi ostacoli, diventa importante selezionare soluzioni tecnologiche compatibili e collaborare con fornitori che comprendano e supportino gli obiettivi di convergenza della sicurezza.

Infine, la valutazione dei rischi e delle priorità è un elemento essenziale della convergenza della sicurezza. Per garantire che le risorse siano allocate in modo efficace, le aziende devono affrontare un processo complesso che richiede di bilanciare le esigenze di sicurezza fisica e informatica e determinare come affrontare le minacce emergenti. Con un'attenta valutazione, le organizzazioni possono assicurarsi di concentrarsi sulle aree più critiche e di proteggere adeguatamente le loro risorse e infrastrutture.

Affrontare queste difficoltà richiede un impegno costante da parte delle aziende e una comprensione approfondita delle implicazioni della convergenza della sicurezza. Tuttavia, superare queste sfide può portare a una protezione più efficace delle risorse e delle infrastrutture aziendali, oltre a una maggiore efficienza operativa.

La convergenza della sicurezza offre vantaggi significativi che vanno al di là della mera protezione delle risorse e delle infrastrutture aziendali. Unendo le forze della sicurezza fisica e informatica, le aziende possono rispondere più rapidamente ed efficacemente alle minacce, riducendo il tempo di esposizione e il potenziale impatto di un incidente. Inoltre, la convergenza della sicurezza può contribuire a ridurre i costi operativi e di gestione eliminando la duplicazione degli sforzi e sfruttando le sinergie tra i team e le risorse.

Negli sviluppi futuri l'adozione delle tecnologie emergenti giocherà un ruolo cruciale nel potenziare le capacità delle aziende di affrontare le minacce in modo più efficace. L'intelligenza artificiale e il machine learning, ad esempio, possono apportare miglioramenti significativi nella rilevazione e prevenzione delle minacce in tempo reale. Queste tecnologie consentono l'analisi di grandi quantità di dati e l'individuazione di modelli di comportamento sospetti, permettendo alle organizzazioni di reagire rapidamente alle minacce emergenti.

Allo stesso tempo, l'adozione di tecnologie come l'Internet of Things (IoT) e la blockchain offre nuove opportunità per rafforzare la sicurezza e migliorare l'integrazione tra sistemi fisici e informatici. L'IoT, in particolare, ha portato a un aumento del numero di dispositivi connessi, creando nuove sfide e opportunità per la sicurezza. Le aziende possono sfruttare le informazioni raccolte dai dispositivi IoT per monitorare e proteggere le loro infrastrutture fisiche, oltre a migliorare la sicurezza dei dati e delle comunicazioni.

La blockchain, invece, può fornire soluzioni innovative per garantire la sicurezza e l'integrità delle informazioni. Ad esempio, la blockchain può essere utilizzata per creare registri crittograficamente sicuri delle transazioni, prevenendo la manipolazione dei dati e garantendo la tracciabilità delle informazioni. Inoltre, la blockchain può facilitare la condivisione sicura delle informazioni tra diverse parti, migliorando la collaborazione e l'integrazione tra i team di sicurezza fisica e informatica.

Per sfruttare al meglio queste innovazioni, le organizzazioni dovranno continuare a investire nella formazione del personale, nella cooperazione tra team multidisciplinari e nell'adattamento delle loro strategie di sicurezza alle nuove sfide e opportunità che queste tecnologie emergenti porteranno.

Abbiamo visto come la convergenza della sicurezza rappresenta un punto di svolta nella protezione delle risorse aziendali, con un impatto che va ben oltre i confini tra sicurezza fisica e informatica. Affrontarne le sfide è un investimento fondamentale per le aziende, garantendo una protezione efficace e duratura dei loro asset più preziosi e contribuendo a creare sistema paese più sicuro e affidabile per tutti.

Le minacce cyber non vanno in vacanza: i rischi per le aziende e gli utenti durante il periodo estivo

A cura di Sofia Scozzari

Le vacanze sono un momento di relax molto atteso.

Tuttavia, i criminali informatici non vanno mai in vacanza e sanno di poter contare sul fatto che si tende ad abbassare la guardia durante i periodi di riposo.

Inoltre, viaggiando e facendo maggiore uso di dispositivi mobili, i rischi cyber aumentano, sia per gli utenti che per le aziende.

In questo panorama digitale sempre più complesso, la stagione estiva rappresenta quindi un momento pericoloso dal punto di vista della Cyber Security.

Vediamo quindi le minacce che mettono più a rischio l'azienda durante le vacanze e qualche suggerimento utile per rimediare.

In che modo le vacanze possono rappresentare un rischio per le aziende

I criminali informatici approfittano dei periodi di vacanza in cui le protezioni aziendali sono meno attrezzate, sia per mancanza di personale che per una diminuzione nella vigilanza degli utenti.

Per lo stesso motivo il tempo di rilevamento e di risposta alle minacce informatiche potrebbe aumentare, con ulteriori conseguenze soprattutto se la problematica entra in azienda a causa di un dipendente in vacanza poco accorto.

Infatti, un utente in vacanza con dispositivi aziendali o che accede a risorse aziendali da remoto (e vale anche per il controllo della posta dallo smartphone) può mettere a repentaglio non solo i suoi dati ma anche quelli del datore di lavoro.

Le principali minacce per le aziende:

- **Accesso a sistemi aziendali da reti Wi-Fi non protette:** anche durante i periodi di relax può presentarsi l'esigenza di controllare le email o accedere ai sistemi aziendali. A questo scopo spesso l'opzione più semplice è quella di utilizzare reti Wi-Fi non protette messe a disposizione da hotel, caffè, aeroporti, stazioni o luoghi turistici. Questo però può mettere a rischio le risorse aziendali: tramite queste connessioni poco sicure i criminali informatici possono infatti intercettare il traffico dati e rubare informazioni sensibili o installare malware e applicazioni indesiderate sui dispositivi.

- **Uso di dispositivi pubblici:** utilizzare un dispositivo pubblico necessita di particolare cautela e andrebbe evitato per l'accesso a risorse aziendali. Sul dispositivo potrebbe essere infatti installato un keylogger o un malware che consente di rubare credenziali di accesso.

- **BEC (Business Email Compromise) scam:** questa problematica include tutti i messaggi di testo o e-mail (potenzialmente anche telefonate), che, mascherando la propria provenienza come una fonte affidabile (un superiore, un fornitore, ecc…), puntano ad ottenere informazioni riservate (ad esempio credenziali di accesso) o vantaggi economici (ad esempio il pagamento di una fattura con dati bancari contraffatti). Le BEC scam possono essere molto insidiose e comportare perdite anche molto importanti.

- **Smarrimento o furto di dispositivi:** durante le vacanze, il rischio di smarrimento o furto di dispositivi, in particolare quelli mobili, come smartphone o tablet, ma anche computer portatili, aumenta. Questo comporta seri pericoli in quanto può permettere l'accesso ad informazioni riservate e sensibili, una problematica ancora più preoccupante quando si tratta di dispositivi aziendali o configurati per consentire l'accesso a risorse aziendali.

- **Esternalizzazione dei servizi:** con parte del personale addetto alla sicurezza in vacanza, può capitare che i servizi vengano esternalizzati per garantire un'adeguata copertura. È fondamentale vigilare sui collaboratori esterni e ricordare che potrebbero non essere abituati alle politiche aziendali, mettendo potenzialmente a rischio l'azienda.

- **Phishing e truffe online:** durante il periodo delle vacanze, aumenta il rischio di essere soggetti a phishing e truffe online, in particolare nel caso di promozioni di offerte di viaggi e sconti allettanti.

Alcuni suggerimenti utili

Dopo aver preso in considerazione le minacce che mettono a rischio l'azienda durante i periodi di relax, vediamo i suggerimenti che aiutano a mitigare questi rischi.

a) Prima di partire

- Il primo consiglio è di selezionare attentamente i dispositivi da portare in vacanza, evitando tutto ciò che non si renderà strettamente necessario durante il viaggio, in particolare se si tratta di dispositivi aziendali.

- I dispositivi selezionati vanno aggiornati con tutte le patch di sistema e gli update applicativi disponibili.

- I dati sensibili che non sono strettamente necessari per il viaggio vanno rimossi, per limitare i danni in caso di furti o smarrimento dei device.

- È buona norma eseguire il backup dei dati presenti sui dispositivi, in particolare quelli aziendali, per mettersi al sicuro dal rischio di danni o perdite.

- Proteggere i dispositivi, sia aziendali che personali, con sistemi di autenticazione forte o accessi biometrici.

- Tenersi aggiornati sulle ultime truffe aiuta a mantenere sempre alto il grado di allerta.

b) Durante le vacanze

- Evitare di utilizzare reti Wi-Fi non sicure per attività sensibili, come l'accesso al conto bancario online o a sistemi aziendali, incluso il client di posta. In mancanza di alternative, il consiglio è di utilizzare una connessione VPN (Virtual Private Network) per cifrare il traffico dati e garantire una maggiore sicurezza.

- È importante disattivare le connessioni automatiche Wi-Fi/Bluetooth per evitare di connettersi in automatico e limitare l'utilizzo di risorse pubbliche allo stretto necessario.

- L'uso di dispositivi pubblici dovrebbe essere limitato esclusivamente a servizi che non richiedono alcuna autenticazione e strettamente non aziendali.

- È bene differenziare l'utilizzo dei dispositivi: le risorse aziendali dovrebbero essere gestite solo con device aziendali, mentre quelli personali vanno utilizzati in tutti gli altri casi.

- Se si deve accedere ai sistemi aziendali o utilizzare dispositivi business, è necessario verificare ed installare eventuali aggiornamenti di sistema e applicativi prima di accedere alle risorse.
- Utilizzare l'autenticazione a più fattori (MFA, Multi Factor Authentication) per accedere a risorse e servizi critici è una buona pratica per limitare il rischio di compromissioni.
- Disattivare i servizi di localizzazione quando non sono in uso per evitare di esporre troppe informazioni.
- Non installare software da fonti non verificate.
- Non lasciare i dispositivi incustoditi o sbloccati in luoghi pubblici.
- Non collegare i dispositivi alle stazioni di ricarica pubbliche, o, in alternativa, assicurarsi di utilizzare un cavo di sola ricarica che non trasmetta dati per evitare le possibilità di contrarre infezioni "informatiche".
- Attenzione ai QR code che potrebbero veicolare l'installazione di malware.
- In particolare se si ricoprono ruoli importanti, è bene gestire la propria presenza online e gli aggiornamenti sui Social Media per evitare di fornire troppe informazioni che un cybercriminale potrebbe trovare utile per pianificare eventuali operazioni malevole. Un buon consiglio è sempre quello di non fornire dettagli troppo precisi sulla propria posizione.
- Avvisare immediatamente l'azienda in caso di furti o smarrimenti di device aziendali o in caso di ulteriori problematiche che potrebbero mettere a repentaglio l'azienda.

c) Al ritorno dalle vacanze

- Nel caso in cui ci si sia esposti a rischi, una buona norma è di cambiare password e PIN al rientro del viaggio.
- Ispezionare i dispositivi dopo le vacanze, possibilmente prima di rientrare in azienda, per rilevare eventuali violazioni o problematiche, è una buona pratica che aiuta a mettersi al riparo dal rischio di diffondere malware involontariamente. In caso di necessità il reparto IT dell'azienda saprà certamente offrire i suggerimenti corretti per eseguire al meglio questo controllo.

Conclusioni:

Le vacanze sono un momento di relax, ma è importante non trascurare la Sicurezza Informatica.

Con alcune semplici precauzioni, è possibile ridurre notevolmente i rischi di Cyber Security a cui le aziende sono inevitabilmente esposte durante le vacanze, ricordando che best practices, consapevolezza e prudenza sono le priorità per proteggere non solo il business ma anche la privacy degli utenti.

Le Best Practices da seguire durante le vacanza devono essere definite e condivise con tutto il personale in modo che dipendenti e collaboratori siano preparati a prevenire e gestire eventuali problematiche.

Inoltre, la consapevolezza delle minacce e dei rischi, unita ad un atteggiamento sempre prudente, è essenziale: evitare di abbassare la guardia anche durante i momenti di relax, rappresenta un requisito fondamentale per assicurarsi vacanze più sicure.

Buone vacanze!

Cyber Think Tank Assintel

Prossimo incontro:

18 luglio

Ore 14:30

CYBER
Think Tank
ASSINTEL

Obiettivi:

1. Interazione
2. Integrazione
3. Coerenza
4. Concretezza

Per info scrivi a:

segreteria@assintel.it

Cybersecurity & Digital Trust

A cura di Valentina Sapuppo

1. Introduzione

Negli ultimi tempi l'importanza del ruolo ricoperto dalla cybersecurity è sempre più evidente a fronte dei numerosi attacchi informatici sferrati in tutto il mondo. Il triste scenario bellico russo-ucraino ha messo in evidenza la potenza distruttiva della cyber-war e, certamente, i numerosi attacchi DDoS e ransomware hanno fatto aprire gli occhi ai più che non si erano ancora accorti che, in un mondo quasi totalmente digitalizzato, è necessario proteggere le porte di accesso per non far entrare a casa propria i pirati digitali.

I numerosi report pubblicati dalle maggiori autorità del settore, sulle tipologie di attacco e gli scenari più colpiti, trasmettono un messaggio importante: è necessario sviluppare sempre più Digital Trust, ponendola come obiettivo primario delle moderne strategie di business di cybersecurity a tutela di tutte le parti interessate, Clienti, Fornitori e Autorità.

In questo articolo illustreremo come mai il ruolo della cybersecurity è così importante nella costruzione di una società digitale sempre più sicura, una società digitale che opera nel Web 3.0 e che si affaccia al 6G networks e a nuovi metaversi.

2. Perchè sviluppare una Digital Trust è così importante?

Tra i concetti di business più ambiti vi è certamente la resilienza e la fama del brand.

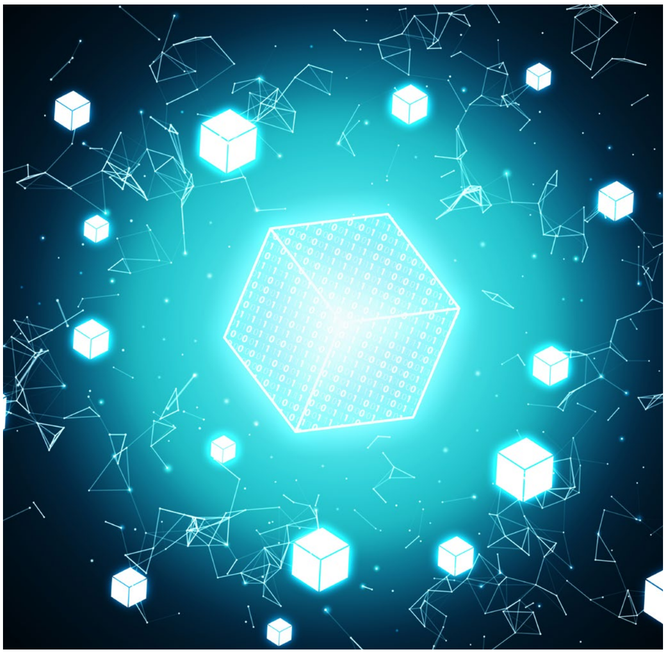
Per le aziende, oggi, non è così semplice garantire il proprio ruolo in un mercato digitale così rischioso. Non sono poche le notizie di aziende molto note che subiscono attacchi informatici e che vedono minata la propria immagine all'esterno e il tutto impatta sulla crescita del business.

Sviluppare la fiducia digitale verso Clienti, Fornitori e Autorità è, quindi, uno dei più ambiti obiettivi delle aziende moderne.

Come fare allora? Nel mondo delle certificazioni ISO/IEC, uno dei requisiti mandatori prescritto è che le aziende - che vogliono accreditarsi secondo uno schema piuttosto che un altro - devono dimostrare di garantire il soddisfacimento delle aspettative delle parti interessate.

Proteggere i dati dei propri clienti o dei propri consumatori genera fiducia. Tutto questo è possibile, però, se le aziende dimostrano di essere capaci di gestire il proprio sistema all'insegna della sicurezza delle informazioni. Così facendo, le aziende si aprono al mondo in cui operano, comunicando all'esterno le proprie politiche di fiducia digitale, garantendo, di conseguenza, la propria reputazione. La gestione del rischio informatico da minacce sempre più sofisticate e vulnerabilità, infatti, può essere soddisfatta solamente se le logiche di business dimostrano un forte interesse nella creazione e nella reale attuazione di una strategia di cybersecurity e di business continuity.

A fronte, però, di tutte accortezze più brillanti è chiaro che il rischio informatico non potrà essere mai annullato del tutto. Nonostante ciò, piani di formazione continua, erogati a tutti i livelli, possono certamente supportare la lotta al fattore umano. Infatti, sviluppare awareness e sensibilizzare tutti gli attori dei processi aziendali è certamente una scelta vincente per mantenere fiducia delle parti interessate.



3. Strategie di Business a supporto della Digital Trust

Mitigare attivamente una vastità indefinita di rischi digitali non è una sfida semplice.

Data breach o data leack, attacchi ransomware o DDoS, sono alcuni esempi frequentemente registrati di difficili lesson learned. Questi alcuni dei motivi per cui è davvero importante sviluppare un concreto e robusto programma proattivo di Information Security a supporto della Digital Trust.

La Threat Intelligence funge da strumento molto utile per comprendere le motivazioni, gli obiettivi e i comportamenti di attacco già subito dagli attori del mercato digitale. Inoltre, l'adozione di best practice e di auto-assessment - come quelli strutturati seguendo gli schemi del CSF NIST o del framework SOC 2, pubblicato dall'American Institute of Certified Public Accountants - AICPA - o l'implementazione di sistemi di gestione ISO/IEC 27001:2022, sono senza dubbio efficaci meccanismi di rinforzo delle politiche e delle procedure operative, realizzati o irrobustiti a valle di un rapporto sui controlli rilevante per la sicurezza, la disponibilità, l'integrità dell'elaborazione delle informazioni, della riservatezza o della data protection e della governance delle informazioni.

Anche l'Unione Europea mette al centro della propria strategia di cybersecurity la Digital Trust.

Infatti, il Digital EU Programme "Shaping Europe's digital future" si propone lo scopo di rinforzare la protezione delle infrastrutture digitali europee a tutela dei cittadini e per il miglioramento continuo della sicurezza dei prodotti e dei servizi digitali.

Con la creazione dell'European Cybersecurity Competence Centre and Network – ECC la Commissione Europea si propone di "unire la sicurezza informatica europea". Infatti, grazie alla collaborazione con i 27 National Coordination Centres - NCCs si persegue l'obiettivo di "promuovere l'eccellenza della ricerca e la competitività dell'Unione nel campo della sicurezza informatica", nonché di aumentare la capacità e la competitività in ambito IT.

4.The EU Cybersecurity Strategy: l'impegno dell'europa per la realizzazione del "Digital europe programme for europe's Digital Transition and Cybersecurity"

È necessario attendere di essere assoggettati a obblighi normativi o, piuttosto, la scelta migliore, nelle logiche di business, è quella di creare un sistema di gestione e sviluppare un concreto e robusto programma proattivo di Information Security a supporto della Digital Trust?

Nel 2022 la Commissione europea e l'Alto Rappresentante dell'Unione per gli affari esteri e la politica di sicurezza hanno presentato una nuova strategia dell'UE in materia di sicurezza informatica. Una chiara presa d'atto della massiva digitalizzazione della società. Nel manifesto, infatti, leggiamo che "l'UE si impegna a sostenere questa strategia attraverso un livello di investimenti senza precedenti nella transizione digitale dell'UE nei prossimi sette anni. Questo quadruplicarebbe i livelli precedenti di investimento."

Il 24 marzo 2023 la Commissione Europea ha adottato due programmi di lavoro pluriennali per la realizzazione del Digital EU Programme for Europe's Digital Transition and cybersecurity - DEP per il biennio 2023/2024, con i quali ha stanziato finanziamenti per 1,3 miliardi di euro, di cui 553 milioni di euro già disponibili nel 2023 per supportare investimenti strategici nel decennio digitale europeo. Il programma vanta il pregio di perseguire il rafforzamento delle capacità digitali critiche dell'Unione, mettendo al centro le aree centrali dello sviluppo digitale europeo, quali la "protezione del clima e dell'ambiente, dei dati, dell'intelligenza artificiale, del cloud, della sicurezza informatica, delle competenze digitali avanzate.” Il DEP è valido anche per PMI e per le start-up non soggette alla disciplina della Direttiva NIS2 e del Cyber Resilience Act – CRA.

Inoltre, la Commissione europea ha creato il Cybersecurity Atlas, una “piattaforma di gestione della conoscenza per mappare, categorizzare e stimolare la collaborazione tra esperti europei di sicurezza informatica a sostegno della strategia digitale dell’UE”. In questa, tra i network pilot projects segnaliamo il Progetto CONCORDIA, ECHO, SPARTA and CyberSec4Europe dal quale è nato l’European Cyber Competence Network.

5. Conclusioni

In questo articolo abbiamo illustrato i motivi per cui il ruolo della cybersecurity è così importante nella costruzione di una società digitale sempre più sicura. La costruzione della Digital Trust è uno degli obiettivi primari delle aziende moderne che perseguono il fine di soddisfare le aspettative delle parti interessate. Inoltre, abbiamo visto come la condivisione di obiettivi di sicurezza informatica è al centro della strategia europea. Security Zero Trust, trasparenza, interoperabilità, resilienza, sicurezza delle informazioni e data protection sono alcune delle parole chiave che dominano il tema trattato. In un mondo sempre più interconnesso è necessario, pertanto, che le aziende prendano decisioni importanti per rendere sempre più affidabili propri prodotti e servizi, dimostrando di saper gestire le informazioni e i rischi IT, all’insegna delle logiche di cyber governance e di risk e vulnerability management.

Prevenire per non subire

Prepararsi ad un attacco informatico può consentire di evitare o mitigare il rischio di doverlo fronteggiare davvero.

A cura di Vittorio Orefice

Tutti noi speriamo e ci auguriamo che non succeda mai all'azienda nella quale lavoriamo, ma, come dicevano i latini: "si vis pacem para bellum", ossia "se vuoi la pace prepara la guerra", che rapportato al nostro tema vuole ricordarci la necessità di dotarsi degli strumenti (informatici ed organizzativi) giusti per essere pronti a difendersi all'occorrenza.

Essere preparati, conoscere ed esercitarsi a adottare le procedure corrette per prevenire, gestire e superare un attacco informatico è oggi di fondamentale importanza per tutte le aziende

Si stima che, almeno in larga maggioranza, le aziende sottostimino questa tipologia di rischio e adottino, di conseguenza, contromisure preventive minimali o insufficienti.

Così abbiamo pensato di raccontare, creando un case study ironico, cosa può accadere per aiutare tutti a valutare meglio quali strumenti utilizzare, per evitare di inoltrarsi in comportamenti a rischio.

Proviamo allora a sviluppare, con l'aiuto di una narrazione astratta, ma vicinissima a molti casi reali accaduti, un caso di attacco informatico con sottrazione o compromissione dei dati ad una PMI italiana.

A questo punto forniamo un dato: di solito chi viene attaccato rimane ignaro dell'accaduto per lungo tempo: si stima che in media l'attacco si palesi dopo 3 o 6 mesi.

In particolare, i tempi più lunghi sono "riservati" a chi non viene direttamente danneggiato, ma solo sfruttato come trampolino per altri assalti. Questo attacco pare meno grave, da certi punti di vista, ma ha pesanti risvolti legali a causa dell'incuria che, colposamente, ha consentito che il criminale danneggiasse altri attraverso le infrastrutture del malcapitato.

L'altro tipo di parte lesa è l'effettivo destinatario di un attacco con sottrazioni e compromissioni di dati ed è la storia che stiamo per raccontare.

Prima di passare alla "storiella" un paio di domande di auto-valutazione.

1. Sospetto per qualsiasi ragione una emergenza sui dati: so che allarme attivare?
2. Sono l'incaricato di reagire ai pericoli: ho un elenco di supporti da contattare?
3. Sono il CEO: so cosa aspettarmi e da chi, ma anche cosa dire e a chi?
4. In azienda sono chiari i doveri delle varie figure in un caso del genere?
5. Si è fatta mai una policy sulla reazione o una simulazione di emergenza?
6. E, buon ultimo, ci sono **backup recenti** e **verificati** delle macchine coinvolte?

Se qualcuna di queste domande vi ha fatto pensare: "ma noi mica siamo la Nasa" o "ma perché dovrebbero attaccare noi", la vostra azienda ha un problema e sta correndo dei seri rischi.

Scopo di questo scritto è convincere ogni azienda ad alzare le proprie difese al massimo che il budget permette. Non ci sono ricette buone per tutti.

Vi suggeriamo di leggerlo provando, dopo ogni passo, a prevedere il successivo momento vissuto dai protagonisti e le decisioni da prendere.

Nel racconto dei **giorni di crisi** che segue scriveremo, come se raccontassimo una storia realmente accaduta all'azienda **del lettore**, è un espediente narrativo per facilitare l'immedesimazione.

Giorno 0: Il rilevamento

La crisi ha inizio con il rilevamento dell'attacco. Il sistema di sicurezza, attraverso segnali anomali, avverte che qualcosa non va.

Si è subìto un data breach: letteralmente una breccia nella difesa perimetrale, anche se oggi il concetto di perimetro è vago, che permette di fare danni all'interno.

Dati aziendali e di persone interne e di clienti sono stati sottratti o criptati o...

Non è il momento del panico, ma dell'azione prevista e ben codificata.

Primo passo: isolare il sistema infetto, per limitare la diffusione del danno. Comunicare immediatamente alla squadra IT e attivare il piano di risposta alle emergenze, se disponibile.

Giorno 1: Richiesta di supporto

È fondamentale cercare aiuto da esperti in materia di cybersecurity per iniziare la remediation e la mitigation. Questi professionisti conducono un'analisi forense digitale per comprendere la natura e l'ampiezza dell'attacco, identificando il tipo di malware utilizzato e come è penetrato nel sistema.

Giorno 2: Ricerca delle cause

Questo è un momento cruciale: bisogna identificare la causa del breach, che può risiedere in una vulnerabilità del software (spesso vetusto e/o non aggiornato), in un attacco di phishing riuscito, o in un'azione di un insider malevolo. Questo passaggio non è solo fondamentale per la mitigazione dell'attacco in corso, ma anche per prevenire futuri incidenti di sicurezza.

Giorno 3: il riscatto

In caso di ransomware, può arrivare una richiesta di riscatto per il recupero dei dati.

Si decide di non pagare.

Non c'è garanzia che, una volta pagato, i dati verranno restituiti. Inoltre, pagare incoraggia gli attaccanti a continuare con le loro azioni illecite.

Giorno 4: Comunicazioni obbligatorie

Occorre(va) notificare l'incidente alla competente Autorità di Protezione dei Dati nel più breve tempo possibile e, comunque, entro 72 ore. Questo è un obbligo imposto dal GDPR. Se l'incidente comporta un alto rischio per i diritti e le libertà dei soggetti coinvolti, bisogna informare anche loro senza ingiustificato ritardo.

Spesso però, accade al giorno 4 o anche più tardi, ma 72 ore sono 3x24 quindi aumenta il rischio di sanzioni!

Giorno 5: Gestione della comunicazione esterna

Bisogna comunicare l'evento ai clienti e partner. È fondamentale mantenere la trasparenza, fornendo informazioni chiare su cosa è successo, quali dati sono stati sottratti e quali misure si sono adottate. Serve equilibrio: non bisogna divulgare dettagli che potrebbero mettere ulteriormente a rischio la sicurezza del sistema, però i comportamenti reticenti o poco chiari sono fortemente controproducenti per la fiducia.

Giorno 6: Recupero e prevenzione

Dopo aver gestito l'attacco e le sue conseguenze imme-

diate, è il momento di guardare avanti. Tutte le vulnerabilità, anche quelle incolpevoli, vanno affrontate e si deve controllare che le misure di sicurezza siano state migliorate per prevenire attacchi futuri.

Il primo giorno dopo la crisi, le riflessioni e le conseguenze.

La gestione di un attacco informatico è una sfida che richiede prontezza, competenza e trasparenza. Sebbene la prevenzione sia sempre la migliore strategia, sapere come reagire a un attacco può fare la differenza tra un incidente contenuto e una crisi devastante. L'importanza di un approccio sistematico e metodico non può essere sottovalutata.

E il momento di analizzare l'errore che ha scatenato/permesso/agevolato la crisi e le altre debolezze che ne permetterebbero di nuove.

Siamo ottimisti, l'azienda della nostra storiella è tra quelle fortunate che sopravvivono alla bufera e, anzi ne escono in certo qual modo rinforzate.

Dopo l'esperienza sanno bene cosa hanno passato e non ci vogliono ricadere.

In questa azienda il Budget per la sicurezza ICT e per la formazione degli utenti subisce aumenti non solo significativi ma potenti. Gli addetti comprendono bene che avrebbero potuto essere disoccupati e non voglio ritrovarsi nuovamente a rischio.

Insomma, sembrerebbe una storia a lieto fine ma come le favole ha un forte scopo formativo!

L'obiettivo di questo articolo è aiutare chi legge a fare propria sin d'ora la condizione virtuosa che subentra, di norma, "dopo l'attacco", tra i fortunati che hanno superato la tempesta.

In sostanza suggeriamo di apprendere dall'esperienza altrui senza averne riportato i danni.

Desideriamo far comprendere al management che la sicurezza aziendale (ICT, ma non solo) e la prevenzione dei rischi in senso lato, costituiscono una best practice per mettersi al riparo da crisi simili, che spesso sono esiziali per i colpiti e, anche se finiscono bene, hanno costi davvero preoccupanti.

Vorremmo che, in qualche modo, questo articolo fosse sufficientemente coinvolgente e così "scioccante" da fungere da monito e indurre a porsi, seriamente, una domanda: la mia azienda ha adottato delle policy aziendali adeguate a prevenire e/o mitigare il rischio di un attacco informatico?

Bibliografia e sitografia

1. Clusit, 2023.
2. R. Razzante, 2023.
3. R. Razzante, 2023.
4. A. Rociola, 2023.
5. E. Filadelfio, 2021.
6. M. Iaselli, G. B. Caria, 2023.
7. N. Caranti, 2020.
8. J. K. Davis, 2022.
9. D. Dell'aria, Direttive NIS 2 e CER, 2023.
10. F. Sarzana Di Sant'ippolito, I.O. Epicocco, M. Pierro, 2022.
11. Considerando, 75.
12. https://medium.com/cycraft/prometheus-decryptor-6933e7bac1ea
13. https://securityintelligence.com/posts/ransomware-encryption-goes-wrong/
14. https://securityintelligence.com/posts/ransomware-encryption-goes-wrong/
15. http://sonarmsniko2lvfu.onion/?a=docs-api
16. https://www.secureblink.com/cyber-security-news/mexican-govt.-data-publicized-with-new-ransomware-group-prometheus-and-grief
17. https://www.secureblink.com/cyber-security-news/mexican-govt.-data-publicized-with-new-ransomware-group-prometheus-and-grief.
18. https://www.kelacyber.com/kelas-100-over-100-september2020-in-network-access-sales/.
19. https://howtofix.guide/prom-virus/
20. P. Laurano, G. Anzera, 2017
21. D. Tosini, 2005
22. D. Tosini, 2005, p 31
23. https://www.senato.it/service/PDF/PDFServer/BGT/908856.pdf
24. https://www.wired.com/story/israel-water-utility-hack-cloro/
25. https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

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 magazine 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.

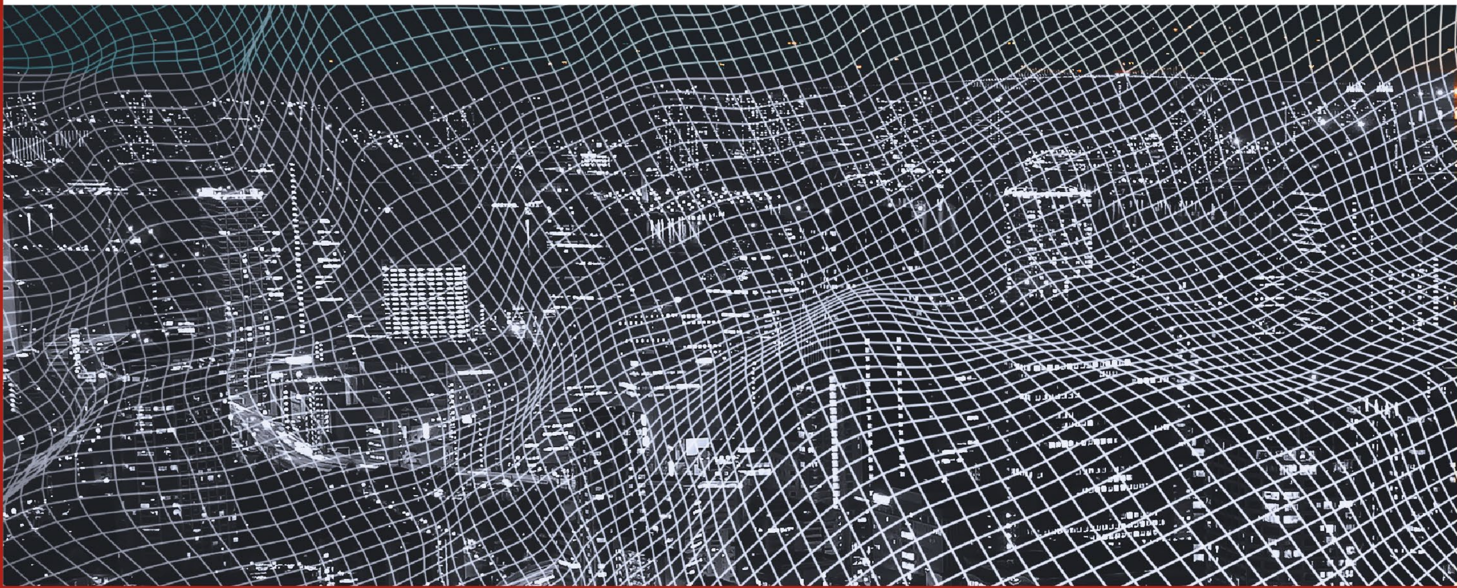
Cordialmente

La redazione

CYBER
Think Tank
ASSINTEL

CYBER MAGAZINE

Giugno - Luglio
2023



Cyber Think Tank Assintel

Contattaci:

segreteria@assintel.it
www.assintel.it