CYBER MAGAZINE

Anno4 / Numero 6
2023

ASSINTEL CYBER SECURITY

ASSINTEL
ASSOCIAZIONE NAZIONALE
IMPRESE ICT

In questo numero:

COORDINATORE:

Pierguido Iezzi

COMITATO SCIENTIFICO:

Antonio Assandri, Gianpiero Cozzolino, Vittorio Orefice

REDAZIONE:

Federico Giberti, Melissa Keysomi, Daniela Grossi

INDICE

L’editoriale del Presidente Assintel Paola Generali

Maggio 2023

Il tema della cybersecurity sta finalmente uscendo da una nicchia di addetti ai lavori e di Cassandre inascoltate per diventare uno degli asset su cui è inevitabile porre l’attenzione su tutti gli ambiti: nel fare impresa, nella Pubblica Amministrazione, nelle strategie geopolitiche, e in generale a livello culturale.

Siamo in una società digitale e data-driven: i temi quindi non possono restare chiusi nei laboratori di ricerca e sviluppo delle aziende specializzate, ma devono poter coinvolgere imprenditori, decisori, tecnologi perché è da loro che può partire una nuova cultura organizzativa che metta al centro la sicurezza in tutte le sue forme.

Questa è l’anima del nuovo Cyber Magazine di Assintel. E’ il frutto del lavoro del nostro Think Tank dedicato alla security, che con la nuova consigliatura è guidato dal collega e amico Pierguido Iezzi, insieme alle tante aziende e contributors che vi partecipano.

Buona lettura,

Paola Generali

ASSINTEL
ASSOCIAZIONE NAZIONALE
IMPRESE ICT

ASSINTEL
CYBER
SECURITY

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

Maggio 2023

È un onore presentarvi il primo numero del 2023 del Cyber Magazine del Cyber Think Tank Assintel.

La sicurezza informatica è un tema sempre più importante per le aziende di ogni dimensione e il Cyber Think Tank Assintel si pone come un importante hub di collaborazione in cui aziende e professionisti possono confrontarsi e affrontare insieme le sfide più pressanti in materia di sicurezza informatica.

Il nostro obiettivo è quello di fornire alle aziende gli standard, le best practice e le migliori tecnologie disponibili in commercio per garantire la sicurezza delle loro informazioni e dei loro dati.

In questo primo numero del 2023, vi invitiamo a scoprire gli ultimi sviluppi in materia di cyber security: dalle minacce più recenti ai nuovi strumenti e tecnologie utilizzati per proteggere i dati delle aziende.

Siamo convinti che la condivisione delle conoscenze sia fondamentale per contrastare le minacce informatiche sempre più sofisticate, e siamo fieri di poter offrire questo spazio di collaborazione e informazione a tutti coloro che sono impegnati in questo campo.

Buona lettura,

Pierguido Iezzi

ASSINTEL
ASSOCIAZIONE NAZIONALE
IMPRESE ICT

ASSINTEL
CYBER
SECURITY

L'evoluzione del social engineering al tempo di ChatGPT

A cura di Pierguido Iezzi

Le TTP (Tecniche, Tattiche e Procedure) utilizzate dai Criminal Hacker sono in costante evoluzione, tanto da evolversi e progredire a pari passo con il ritmo del progresso tecnologico. Va da se, quindi, che l'arrivo di strumenti commerciali di intelligenza artificiale possano rappresentare per questo gruppo di antagonisti digitali un'opportunità di migliorare e perfezionare l'arsenale a loro diposizione. In particolare, nel campo del social engineering.

Storicamente, gli attacchi di social engineering portano in corredo alcuni segnali di riconoscimento inequivocabili; che l'utente medio è oramai abbastanza avvezzo a notare.

Strani saluti, nomi sbagliati, grammatica scorretta o molto meccanica, richieste confuse e ad alta priorità: questi sono alcuni dei famigerati segni distintivi di un'e-mail di phishing che tutti abbiamo imparato a riconoscere e che ci permettono di alzare gli occhi al cielo, cancellare il messaggio e andare avanti con la nostra giornata.

Ma i nuovi progressi nel campo dell'intelligenza artificiale stanno eliminando questi indicatori evidenti, rendendo sempre più difficile per gli utenti – e a volte anche per i professionisti - distinguere tra un'e-mail legittima e una di phishing, lasciando le aziende esposte.

ChatGPT, oramai "la celebrità" in questo campo, si appresta potenzialmente a modificare in modo permanente le regole del social engineering.

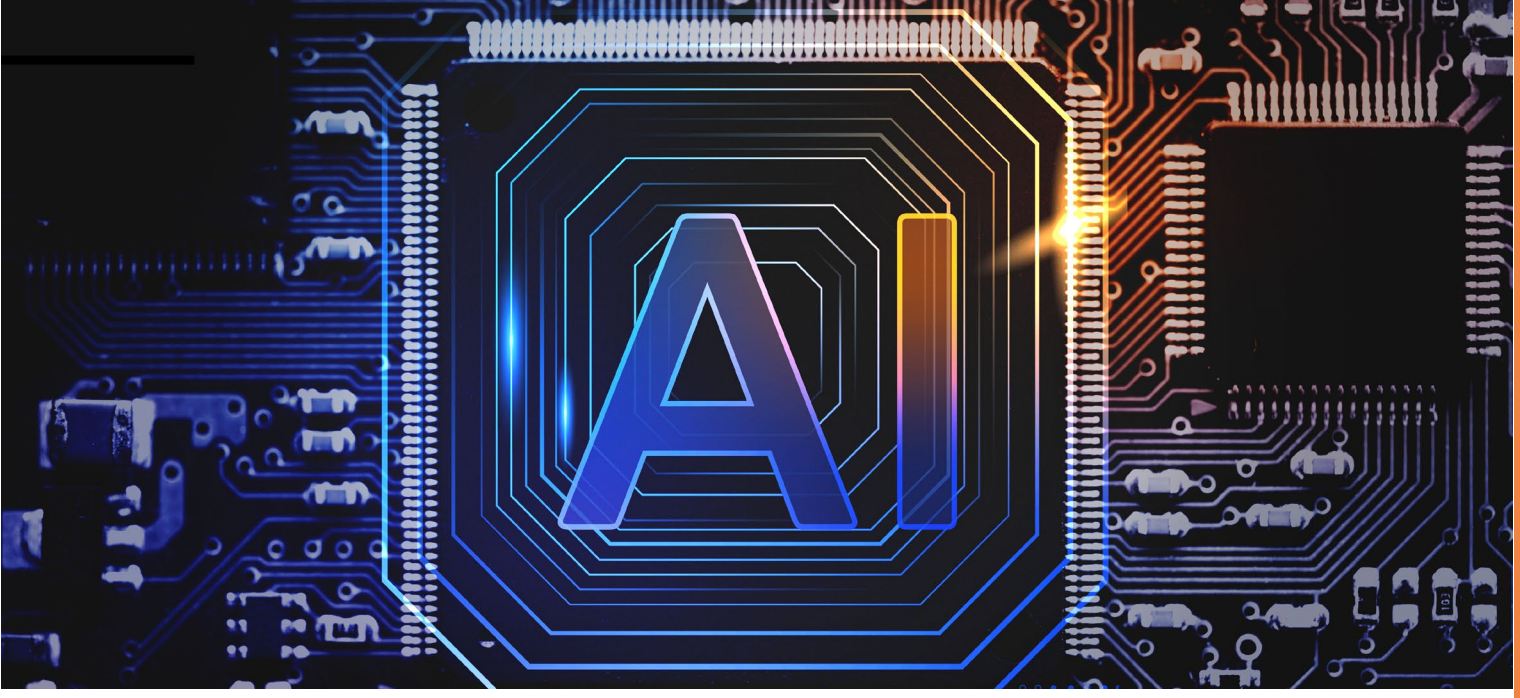
L'arrivo del prodotto di Open AI è diventato protagonista delle prime pagine della cronica, suscitando anche un turbine di incertezze sull'impatto che potrebbe avere sul panorama della cybersicurezza.

Sebbene gran parte della conversazione sia stata sensazionalizzata, il suo impatto sulle campagne di phishing è molto reale.

ChatGPT è un modello generativo programmato per imitare la conversazione umana, redigere contenuti di lunga durata, comporre musica e persino scrivere e correggere codice.

Quest'ultima capacità ha suscitato molta attenzione nella comunità informatica, in particolare quando si prende in considerazione la possibilità della comparsa di malware scritti da ChatGPT.

Tuttavia, la chatbot rappresenta un'altra minaccia che è stata inizialmente un po' trascurata nell'discorso intorno a questa soluzione: le e-mail di phishing generate dall'intelligenza artificiale.



ChatGPT consente ai Criminal Hacker di infondere nelle loro e-mail di phishing capacità comunicative che storicamente non sono state il loro punto forte, in particolare quando si tratta di messaggi in lingue che non siano l'inglese.

Utilizzando questo chatbot, è possibile produrre gratuitamente e-mail di phishing coerenti, colloquiali e indistinguibili dai messaggi legittimi, il che significa che anche il criminale informatico più rudimentale può migliorare i propri attacchi di social engineering.

Sono finiti i tempi in cui un nome scritto male o una grammatica approssimativa potevano destare preoccupazione. Sebbene ChatGPT disponga di controlli per prevenire questo tipo di abuso, è facile per un attore delle minacce manipolare la soluzione semplicemente riformulando la richiesta in modo da evitare qualsiasi frase allarmistica.

Un altro modo per aggirare le linee guida di ChatGPT è quello di utilizzare lo strumento per perfezionare le e-mail di phishing preesistenti e già in circolazioni.

Il risultato di questo lavoro di "lucidatura" potrebbe benissimo ingannare anche l'utente più esperto e indurlo a fare clic su un link sospetto, con conseguente aumento degli attacchi di account takeover e business email compromise.

Le conseguenze di questa evoluzione le conosciamo: danni finanziari, danni reputazionali e possibili rischi di escalation sui sistemi colpiti.

Detto questo, non dobbiamo dimenticare che ad oggi, il social engineering più avanzato, richiede comunque ancora una componente umana.

Mentre i Criminal Hacker, come abbiamo illustrato, potrebbero usare ChatGPT per scrivere messaggi convincenti o tradurre le loro esche nella lingua nativa delle vittime - essenzialmente usando la chatbot per scrivere un messaggio che suoni più vicino alla lingua nativa di quanto possa fare Google Translate, questo funziona solo in campagne di phishing generiche o a strascico (il classico messaggio del corriere o di uno dei colossi dell'e-commerce).

L'AI, per il momento, perfeziona, ma non evolve necessariamente.

I Criminal Hacker veramente specializzati in Social engineering, ancora oggi, operano studiando il modo in cui le loro vittime comunicano, sia internamente tra di loro che con i partner e i clienti esterni.

Imparano a imitare o impersonare colleghi e i clienti, a usare il gergo giusto e quindi a ingannare con maggior successo il personale per farsi consegnare credenziali, credenziali di accesso o persino denaro tramite bonifici.

Exploit e vulnerabilità, sono normali, ma il social engineering sofisticato è qualcosa che non si trova tutti i giorni. E, soprattutto l'AI non né è – ancora – responsabile.

Blockchain e Pubblica Amministrazione

A cura di William Nonnis

Nell'ottobre 2008, Satoshi Nakamoto, lo pseudonimo dietro il quale si cela l'identità del creatore di bitcoin, pubblica il white paper "Bitcoin: A Peer-to-Peer Electronic Cash System". In questo documento, Nakamoto descrive la tecnologia alla base della **criptovaluta,** che utilizza una rete peer-to-peer per consentire il trasferimento di valore senza la necessità di intermediari finanziari.

La prima transazione in bitcoin viene effettuata il 12 gennaio tra Satoshi Nakamoto e Hal Finney, un noto esperto di crittografia.

Vale la pena notare che l'hash della transazione del primo bitcoin contiene il testo "The Times 03/ Jan/2009 Chancellor on brink of second bailout for banks".

La "moneta elettronica" che ha fatto da apripista alla cryptocurrency, oltre che apportare un modo del tutto nuovo di intendere l'economia, in virtù della DeFi - la finanza decentralizzata - ha generato anche un'altrettanto straordinaria innovazione per il nostro tempo: la Blockchain.

Nato come necessario sostegno tecnologico per veicolare online le criptovalute, tale protocollo ha mostrato ben presto le sue dirompenti potenzialità di utilizzo anche in contesti differenti dal settore economico/finanziario.

La Blockchain può essere assimilata a un libro mastro digitale, un registro pubblico di dati, inseriti previo consenso dei partecipanti al network che, in modo autonomo e indipendente, effettuano in rete la registrazione.

Ogni nodo della catena, vale a dire ogni partecipante che contribuisce alla validazione dell'informazione (la quale avviene solamente con il 50% più uno del consenso, su migliaia di nodi), ha lo stesso identico peso e valore ai fini della validazione e ciò costituisce il cuore fondante di tale tecnologia che, proprio per la mancanza di un sistema apicale di controllo, risulta essere un Sistema Distribuito (Distributed Ledger).

Dalla totale decentralizzazione deriva la trasparenza dei dati immessi e, cosa più importante, la loro immutabilità, motivo per cui la Blockchain è uno strumento potentissimo di gestione e conservazione delle informazioni iscritte, non suscettibile a manomissioni o alterazioni di alcun tipo.

Essendo inoltre i nodi di una rete, distribuiti su tutto il globo tecnologizzato ed essendo operativi in maniera anonima, risulta impossibile da praticare

ogni forma di interazione/corruzione sulla loro attività, motivo per cui lo slogan "don't trust, verify", in voga tra gli entusiasti della tecnologia Blockchain, ben corrisponde alla solidità di un sistema di registrazione, granitico nella sua affidabilità.

Non in ultimo, data l'esplosione del cybercrime di attacchi hacker, che in Italia negli ultimi otto anni ha avuto un incremento del 72%, converrà sapere che la rete Blockchain non può essere attaccata in virtù del fatto che, qualora venisse hackerato un nodo, l'intera catena non ne subirebbe alcun effetto, proseguendo inamovibile il proprio percorso di validazione.

Ciò avviene perché, i dati inseriti con un sofisticatissimo sistema crittografico, sono suddivisi in blocchi concatenati e immessi in ordine cronologico, cosicché se un nodo per un qualsiasi motivo non dovesse partecipare alla transazione, si procede con quello successivo e, se manomesso con l'inserimento di un dato fallace, la validazione dell'informazione sbagliata, come detto, dovrebbe estendersi alla metà più uno dei nodi validatori, cosa ovviamente impossibile da realizzare.

Altresì, i dati iscritti non solo non sono manipolabili, ma neanche cancellabili, rendendo in tal modo ogni informazione transata in Blockchain come incisa su pietra, pubblica e inalterabile nel tempo.

Per tutte queste caratteristiche, la Blockchain si presta a offrire garanzia di certezza in tutte quelle attività in cui sia necessario un dato correttamente certificato ed è nelle pratiche della Pubblica Amministrazione che tale tecnologia può trasformarsi nel volano per rendere il sistema Paese agile, moderno ed affidabile.

Infatti, i farraginosi ingranaggi della burocrazia, che ancora oggi rallentano l'iter dell'utente che si rivolge alle istituzioni per l'espletamento di una qualche pratica, sono facilmente superati con la Blockchain, che rende immediatamente disponibile e a portata di click ogni informazione già in essa certificata e quindi assolutamente certa.

Il primo, macroscopico corollario per una PA che utilizza il registro distribuito digitale, con le sue caratteristiche di trasparenza e tracciabilità, è l'innalzamento della qualità dei servizi resi al cittadino, poiché un maggiore monitoraggio dei

propri dipendenti, dato dalla possibilità di visualizzare le pratiche svolte e le tempistiche per singola procedura, può consentire degli incentivi alle risorse più meritevoli, con la diretta ricaduta di una maggiore fiducia nella macchina pubblica da parte dell'utenza.

Sicuramente gli ambiti della PA che investono la quotidianità di ogni cittadino, sono quelli che possono usufruire più e meglio della Blockchain.

In primis la Sanità, finalmente in grado di creare per ogni cittadino un continuum digitale con tutto il suo storico sanitario e con chiavi per decrittografare le informazioni mediche in suo possesso, così da poter scegliere a chi, come e quando mostrare i propri dati. E non solo con benefici per la privacy, che soprattutto in ambito medico è argomento di cruciale importanza, ma per evitare la dispersione dei dati e sanare l'annosa mancanza di comunicazione tra le varie aziende ospedaliere, anche internazionalmente.

Il settore della distribuzione energetica, altro ambito "caldissimo" per tutta la popolazione, grazie alla rete Peer to Peer in Blockchain, è in grado di conseguire il doppio e importante beneficio di un consistente risparmio per l'utente, che può vendere la sua energia in eccesso, favorendo contemporaneamente un utilizzo più responsabile e privo di spreco delle risorse energetiche.

Persistendo sulla via del Self-Sovereign Identity (SSI), ossia sull'identità digitale decentralizzata, che restituisce il possesso e il controllo all'utente dei propri dati personali, con la Blockchain si può superare il limite delle diverse tipologie di documenti di riconoscimento, affidati a terze parti (vedi lo SPID), perché sarà proprio l'utente a generare automaticamente, tramite crittografia, il proprio identificativo, senza più necessità di alcuna autorizzazione e/o rinnovo.

Il brevissimo excursus sui benefici della Blockchain nella PA, finora fatto, andrebbe ampliato, trattando anche delle diverse ramificazioni da cui si generano a macchia d'olio vantaggi in settori che si intersecano tra loro, perché con la digitalizzazione ogni ambito non è più un comparto stagno, ma liquidamente, si mescola e fonde con altri settori.

Difendere l'azienda dai rischi: chi deve pensarci e perché?

A cura di Vittorio Orefice

Iniziamo da un dettaglio di notevole importanza: la parola sicurezza ha tanti significati. A seconda del contesto e della formazione di chi parla, possiamo pensare alla difesa fisica, al controllo sulla proprietà intellettuale, alla volontà di non compiere reati contro l'ambiente, alla protezione dal phishing o alla prevenzione di scalate ostili in borsa.

La sicurezza può essere definita come lo stato di protezione e di assenza di pericolo o minaccia a cui è soggetto un individuo, una comunità o un'organizzazione.

In corsivo ne vogliamo richiamare bene il concetto. Siamo sicuri che il lettore non mancherà di trovare almeno qualcuno degli aspetti, se non nuovo, spesso disatteso nella sua realtà aziendale.

In generale, la sicurezza si riferisce alla capacità di prevenire, ridurre o gestire i rischi e le minacce che possono mettere a repentaglio l'incolumità, la salute o il benessere di un individuo, di una comunità o di un'organizzazione. La sicurezza può essere ottenuta attraverso l'adozione di misure preventive, come l'implementazione di sistemi di controllo e di monitoraggio, la formazione del personale, l'adozione di protocolli e procedure di sicurezza, la definizione di piani di emergenza e di continuità delle attività in caso di crisi o di attacchi.

Inoltre, la sicurezza implica anche la capacità di reagire in modo efficace e tempestivo in caso di emergenza, per minimizzare i danni e ripristinare il normale funzionamento delle attività. Questo aspetto della sicurezza è spesso chiamato sicurezza reattiva.

In ogni contesto, la sicurezza deve essere valutata in base ai rischi specifici a cui è soggetto l'individuo, la comunità o l'organizzazione. Ciò significa che le misure di sicurezza adottate devono essere proporzionate alla natura e alla gravità dei rischi, e devono essere continuamente riviste e aggiornate

per garantire la massima efficacia e protezione possibile.

In sintesi, la parola sicurezza si riferisce alla protezione e alla prevenzione dei rischi e delle minacce a cui è soggetto un individuo, una comunità o un'organizzazione. Essa implica l'adozione di misure preventive e reattive, proporzionate alla natura e alla gravità dei rischi, e deve essere continuamente rivista e aggiornata per garantire la massima efficacia e protezione possibile.

Essa può essere declinata in diversi ambiti, ad esempio la sicurezza personale, la sicurezza informatica, la sicurezza alimentare, la sicurezza del lavoro, la sicurezza stradale e così via.

Come si vede con pochissimi flash in ambiti differenti abbiamo facilmente dimostrato che la sicurezza è un concetto trasversale e avvolgente, ma continuando dimostreremo che contiene sia il concetto di sbarramento passivo nei confronti degli attacchi che quello di ripresa dell'operatività in caso di attacco subìto e, purtroppo, non bloccato.

Quindi non possiamo liquidare questo aspetto,assai critico, della vita aziendale come se fosse (spesso viene posto in questi termini) una piccola parte, secondaria e misconosciuta, dei compiti dell'ICT.

La sicurezza aziendale è invece un tema cruciale per qualsiasi azienda, e coinvolge tutte le figure manageriali, non solo l'ICT: se ciascuna area farà in modo privo di rischi il suo lavoro l'azienda intera vedrà ridursi il rischio.

Tuttavia per brevità e nel rispetto del nostro ambito consulenziale ci limiteremo a discutere le problematiche e le tecnologie che in qualche modo riguardano la sfera informatica.

L'importanza della sicurezza aziendale non può essere sottovalutata, poiché gli attacchi informatici sono sempre più sofisticati e le conseguenze di un attacco possono essere molto gravi, sia in termini economici che reputazionali.

Per questo motivo, è fondamentale che la sicurezza aziendale sia un valore tenuto in considerazione da tutti i collaboratori dell'azienda, sia interni che esterni. Non solo i dipendenti, ma anche i partner commerciali e i fornitori devono essere consapevoli dell'importanza della sicurezza aziendale e collaborare per garantirla. L'azienda deve vigilare, attivamente, sul rispetto delle regole da parte dei partner.

Ad esempio, se l'azienda utilizza un fornitore di servizi

cloud, deve assicurarsi che il fornitore rispetti gli standard di sicurezza e che le credenziali di accesso siano gestite in modo sicuro. Inoltre, l'azienda deve accertare che tutto il personale coinvolto sia formato adeguatamente sulla sicurezza informatica.

Quanto sopra deve avvenire mediante un processo formale e supportato da documenti (NDA ed altro) che permettano all'azienda di rivalersi in caso di danni prodotti o derivanti da incuria di terze parti.

Le figure manageriali hanno un ruolo fondamentale nel garantire la sicurezza aziendale. I manager devono avere una conoscenza approfondita dei rischi informatici e delle best practice per prevenirli. Devono inoltre assicurarsi che le politiche di sicurezza aziendale siano correttamente applicate e che il personale sia formato in modo adeguato.

Inoltre, i manager devono collaborare con gli esperti di sicurezza informatica per garantire che l'infrastruttura tecnologica dell'azienda sia protetta. Devono inoltre definire un piano di emergenza per gestire eventuali attacchi informatici e garantire che tutti i dipendenti siano a conoscenza del piano e in grado di attuarlo in caso di necessità.

A ciò si aggiunga che i piani di emergenza destinati a questi casi sporadici (si spera infatti di non doverli mai attivare) devono essere testati periodicamente da un lato per garantire la pronta ed ottimale esecuzione in caso di necessità e dall'altro per affinarli ed aggiornarli.

Ma la sicurezza aziendale non riguarda solo le figure manageriali. Tutti i dipendenti dell'azienda devono essere consapevoli dei rischi informatici e adottare le opportune best practice per prevenirli. Ad esempio, devono evitare di utilizzare password semplici o di condividere le proprie credenziali di accesso con altri, e devono essere in grado di riconoscere eventuali tentativi di phishing. Sia chiaro che il phishing viene qui usato come rappresentante simbolico di tutta la categoria di attacchi social engineering.

Inoltre, i dipendenti devono essere formati regolarmente sulla sicurezza informatica, al fine di garantire che siano a conoscenza degli ultimi rischi e delle migliori pratiche per prevenirli e la loro formazione deve essere asseverata con test periodici volti a garantire la correttezza della risposta aziendale.

In questo modo, l'azienda può garantire la sicurezza dei propri dati e delle proprie infrastrutture tecnologiche, proteggere la propria reputazione e assicurare la continuità delle proprie attività in caso di attacco informatico.

È importante che le aziende investano in formazione e iniziative volte a sensibilizzare il personale sulla sicurezza informatica, al fine di garantire che tutti

i dipendenti siano a conoscenza dei rischi e delle migliori pratiche per prevenirli.

Inoltre, l'azienda deve continuamente monitorare la propria infrastruttura tecnologica per individuare eventuali vulnerabilità e adottare le misure necessarie per correggerle. La sicurezza informatica è un processo continuo e in continua evoluzione e richiede una costante attenzione da parte di tutti gli attori coinvolti.

In sintesi, la sicurezza aziendale è un aspetto critico che coinvolge tutte le figure manageriali e tutti i collaboratori dell'azienda, sia interni che esterni. L'adozione di buone pratiche e l'investimento in formazione e sensibilizzazione sono fondamentali per garantire la protezione dei dati e delle infrastrutture tecnologiche dell'azienda e assicurare la continuità delle proprie attività in caso di attacco informatico.

In conclusione, la sicurezza aziendale è un tema cruciale per qualsiasi azienda, e coinvolge tutte le figure manageriali, non solo l'ICT. Tutti i collaboratori dell'azienda, sia interni che esterni, devono essere consapevoli dei rischi informatici e adottare le best practice per prevenirli. In questo modo, l'azienda può garantire la propria sicurezza passiva.

Vi è ancora da considerare tutto il tema della reazione all' eventuale attacco effettivamente subito che tratteremo in un successivo articolo, che crediamo potrà interessare tutti voi, sul prossimo numero del nostro magazine.

Cyber Think Tank Assintel

Join us!

Progetti 2023

1 Magazine

2 Webinar

3 Directory delle Aziende & Competenze Cyber

4 Threat Infosharing

5 Nuovi Progetti

Come sopravvivere nel moderno scenario cyber grazie alla cybersecurity intelligence

A cura di Ettore Guarnaccia

Il conflitto Russia-NATO in Ucraina si è presto trasformato in una vera e propria guerra cibernetica, con gruppi di cyber criminali, cyber terroristi e hacktivisti, spesso state-sponsored, a darsi battaglia sul piano informatico.

Questa cyberwar ha fatto irruzione in uno scenario già ampiamente preoccupante, in cui da tempo diversi gruppi di cyber criminali prendono di mira obiettivi critici e aziende di vari settori.

Conflitti, terrorismo, criminalità, hactivismo, competizione di mercato e insider minacciano ogni giorno la reputazione del marchio e la continuità e la sopravvivenza del business di numerose aziende, nonché l'erogazione dei servizi primari (elettricità, gas, acqua, telecomunicazioni, trasporti, ecc.) di intere nazioni.

La cronaca riporta una serie impressionante di attacchi di ingegneria sociale e sfruttamento di vulnerabilità per interrompere servizi primari, compromettere dispositivi OT, IoT e sistemi di controllo industriale, ottenere credenziali di accesso, codice software e informazioni sensibili, installare e diffondere malware (infostealer, ransomware o wiper), o supportare l'opera di disinformazione e propaganda mediatica delle parti in conflitto.

Questo scenario globale impone alle aziende di abbandonare la navigazione a vista e iniziare a compiere scelte basate sul rischio, adottando un approccio preventivo e sempre più predittivo, mettendo in atto le migliori contromisure per salvaguardare il proprio business. Uno dei principali problemi è doversi destreggiare tra numerose fonti di dati e informazioni per individuare le minacce più rilevanti e determinarne i rischi, evitando disinformazione e propaganda, escludendo informazioni false o non pertinenti, e verificando l'affidabilità di quelle applicabili al contesto operativo della propria azienda.

Un concetto che trova riscontro anche nei dati stessi che interessano in particolare il nostro Paese. Secondo

il prossimo rapporto sul fenomeno ransomware, realizzato da Swascan, infatti in particolar modo sono a rischio le PMI. Come spiega Pierguido Iezzi, CEO e Co-founder dell'azienda milanese: "L'attenzione delle gang ransomware nei confronti della PMI italiana può essere sicuramente attribuibile alla maggiore facilità nel colpire questo settore. Spesso budget a disposizione non adeguati, minori competenze disponibili e una minore sensibilizzazione del personale sono e rappresentano una opportunità per i criminal hacker. A questo dobbiamo aggiungere che spesso sono proprio queste aziende che cedono al ricatto poiché i sistemi di backup (ultima possibilità per il recupero dei dati) non sono configurati in sicurezza e di conseguenza vengono anch'essi crittografati. Diventano così completamente inermi e spesso il pagamento del ricatto diventa l'unica via per poter riprendere l'operatività del business. Ecco che se da un lato sono un target più facilmente aggredibile sono anche un target che garantisce una maggiore probabilità di guadagno".

"La PMI non ha un ruolo solo economico nel breve termine per queste gang – continua Iezzi - La PMI italiana rappresenta una grossa fetta del prodotto interno lordo, è il nostro vantaggio competitivo italiano. Il loro know-how, i loro brevetti, i loro progetti, in ogni attacco informatico da ransomware, sono anche informazioni che vengono esfiltrate. Dati e informazioni nell'attuale conflitto potrebbero essere anche interessanti per una Russia che ha l'import completamente bloccato. Ecco un ulteriore elemento di attenzione e preoccupazione nazionale. La perdita di questi dati rappresenta a tutti gli effetti un danno competitivo a livello geopolitico nel medio e lungo termine".

Sicuramente, ribadisce l'esperto, è necessario intervenire con aiuti concreti alla PMI, il PNRR potrebbe essere la soluzione ma allo stesso tempo è necessario intervenire legalmente sulla questione del pagamento dei riscatti. Di fatto diventerebbe uno scudo di tutela per le nostre aziende poiché andrebbe a disincentivare gli attacchi legati al cyber crime riducendo drasticamente la possibilità di ottenere un guadagno dagli attacchi informatici.

Cyber security intelligence di fronte al cambiamento

Questa situazione di grande incertezza, conseguenza di pandemia, pressioni economiche e tensioni geopolitiche, induce in molti CEO un grande preoccupazione per la sopravvivenza della loro

azienda, che trasmettono ai rispettivi CISO.

Ed è proprio nell'incertezza che la disciplina della cybersecurity intelligence trova la propria realizzazione, supportando efficacemente l'individuazione delle minacce emergenti e dei rischi cyber per il business, promuovendo la comprensione della natura dei rischi a tutti i livelli decisionali e, quindi, la definizione delle migliori strategie di difesa.

Essa è un processo di raccolta, analisi e correlazione di dati e informazioni relativi sia al business aziendale (marchio, prodotti, servizi, clientela, terze parti, ecc.) sia al comportamento e all'eventuale impatto di potenziali avversari, che possono essere rappresentati da cyber criminali, cyber terroristi e hacktivisti, ma anche da aziende concorrenti senza scrupoli o da soggetti infedeli interni all'azienda.

Il presupposto fondamentale di qualsiasi strategia di difesa, che debba tradursi in azioni tempestive ed efficaci, è la conoscenza approfondita sia dei propri beni e servizi da proteggere, sia dei propri avversari, del loro modo di agire, le loro motivazioni e i loro obiettivi. In un aforisma: *"non puoi proteggere qualcosa che non conosci da ciò che non conosci".*

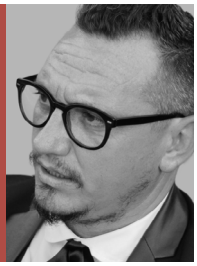
Oggi più che mai è importante porsi le giuste domande. Quali sono i beni e i servizi vitali che reggono il business della mia azienda e che devo salvaguardare a tutti i costi? Quali sono gli avversari che potrebbero avere un interesse ad attaccare la mia azienda e minarne immagine, reputazione e continuità del business? Come agiscono questi avversari e con quale possibile impatto? Quali misure preventive potrei attuare per impedire che eventuali tentativi di attacco non producano impatti per la mia azienda?

Come ho spiegato nel mio ultimo libro ***"Cybersecurity Intelligence"***, una risposta affidabile, efficace e tempestiva a tutte queste domande viene dalla cybersecurity intelligence e dal valore aggiunto che essa può apportare ai processi aziendali di sicurezza e di salvaguardia del business: security operations, incident response, vulnerability management, risk management, controllo della sicurezza delle terze parti, protezione del marchio, geopolitica e consapevolezza del top management e del personale aziendale.

Solo chi investirà sulla conoscenza approfondita della propria azienda e dei suoi avversari può sperare di sopravvivere in questo moderno scenario di minaccia cyber.

La road map dell'intelligence oggi

A cura di Marco Santarelli



Quando oggi si parla di Intelligence, a cosa ci si riferisce esattamente? Per poter rispondere a questa domanda, è necessario prima comprendere tre concetti fondamentali: informazione, comunicazione, rischio. Concetti questi legati a dei passaggi storici essenziali, senza i quali non saremmo arrivati al concetto moderno di Intelligence.

L'informazione nasce con il passaggio di notizie e conoscenze attraverso la narrazione, per evolversi con l'invenzione della stampa nel 1450 circa, arrivando a Internet e alla globalizzazione, che hanno rivoluzionato il modo di comunicare. L'informazione oggi può essere definita come l'organizzazione dei dati raccolti per evitare le fake news, la cui rapida diffusione è alimentata dai social media, dalla loro ampia visibilità e dalla velocità di condivisione dei contenuti, combinati con le emozioni e i sentimenti primari delle persone. Le informazioni sono, allo stesso tempo, fonte di ragionamento e processo decisionale e vengono elaborate in base al contesto. Possono essere di vario tipo: privilegiate, ossia quelle di carattere preciso e non ancora diffuse; pubbliche, le cosiddette news; riservate, quelle divulgabili perché destinate a determinate persone; esterne, quelle che provengono da fonti esterne; interne, quelle provenienti da fonti interne.

La comunicazione, invece, include linguaggio verbale e non verbale, è un medium, un agente di socializzazione. È caratterizzata da codici comunicativi, frutto di una convenzione sociale, ovvero di un patto stipulato tra i membri di una comunità, quindi relativi al popolo e alla cultura, ma è anche un processo di interazione sociale: si ha comunicazione quando qualcuno trasmette qualcosa a un altro. L'emittente di una comunicazione è la fonte di produzione del messaggio, da cui parte l'atto della comunicazione. Il codice, invece, è il sistema convenzionato di riferimento tramite cui il messaggio ricevuto viene decodificato.

Veniamo al concetto di rischio. I Servizi di sicurezza di tutto il mondo hanno sviluppato nel tempo strumenti utili ad ogni analista. Questo meccanismo, di riflesso, ha generato la capacità di una sempre più matura risposta metodologica, logica e tecnica al problema e ha posto condizioni stringenti sulla vita delle persone. Anche il concetto di sorveglianza sta virando progressivamente da pericolo a deterrente

sulla prevenzione e sulle minacce perché in ballo ci sono le nostre stesse vite. Tutto questo, con un pizzico di qualunquismo, possiamo chiamarlo rischio ibrido. Ovvero strumenti per contrastare pericoli di natura molteplice che hanno un'estensione da una parte su fattori esterni, dall'altra su fattori interni. I fattori esterni sono le cosiddette Infrastrutture Critiche o servizi essenziali, ovvero tutti quei "servizi per il benessere della popolazione, la sicurezza nazionale, il buon funzionamento del Paese e la sua crescita economica". I fattori interni sono due: da una parte il rapporto con le persone più prossime (famiglia, colleghi, amici e altro) e dall'altra con quel genio maligno a cui abbiamo dato il nome, a volte impropriamente, di tecnologia. Questi fattori, con i loro strumenti, hanno definito meglio il concetto di Sicurezza, divenuto sempre più interdisciplinare, legato al mondo sociale, a ciò che ci circonda, creando nuove domande su sorveglianza, controllo e protezione.

Intelligence ieri e oggi

Posto questo principio storico e gli assi da cui partire, vediamo come l'Intelligence oggi cambia attraverso una sempre più sensibile attenzione alle dinamiche delle persone e non solo degli Stati. Infatti, in passato per attività di Intelligence si intendevano tutte le attività legate allo spionaggio e al controspionaggio attuate da organismi istituzionali, che si avvalevano di professionalità provenienti da ambienti diversi, che, a loro volta, agivano secondo peculiari procedure volte a salvaguardare la riservatezza degli operatori e delle loro attività. Oggi Intelligence, dal latino, o meglio dalla lingua dei Cesari, intelligere, interpretato nel tempo come inter-legere, leggere dentro o tra, intendere, concepire, comprendere, dire, indica anche attività estendibili ad ogni azione che genera business o che può essere un rischio anche per le aziende. Quindi anche termini come ibrido, minaccia, rischio e così via sono entrati a far parte di queste attività di ricognizione dal "nemico", aspetto che è cruciale anche nelle procure in fase di indagine. Perché è accaduto questo?

Con le due modifiche che sono state applicate alla legge 124/2007 del 3 agosto, "Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto", pubblicata nella Gazzetta Ufficiale n. 187 del 13 agosto 2007, entrata in vigore il 12 ottobre, ampliamento e superamento della nota legge 24-10-1977 n. 801, "Istituzione e ordinamento dei servizi per la informazione e la sicurezza e disciplina del segreto di Stato", l'Intelligence è passata dalla vecchia formula dei due "Servizi per le informazioni e la sicurezza" al "Sistema di informazione per la sicurezza della Repubblica". In questo modo, il raggio d'azione si è ampliato, aprendosi, dall'ambito politico-militare segreto, anche agli altri settori economico, scientifico

e industriale.

Nello specifico, la prima modifica è rappresentata dalla Legge 7 agosto 2012, n. 133, Modifiche alla legge 3 agosto 2007, n. 124, concernente il Sistema di informazione per la sicurezza della Repubblica e la disciplina del segreto, pubblicata nella Gazzetta Ufficiale 10 agosto 2012, n. 186 e entrata in vigore il 25 agosto 2012. Obiettivo di questa normativa è il rafforzamento della protezione delle Infrastrutture Critiche materiali e immateriali, soprattutto in ambito cibernetico e informatico, e delle attività di informazione. La seconda modifica è più recente, è stata applicata, infatti, con il D.L. 30 luglio 2020, n. 83, coordinato con la legge di conversione 25 settembre 2020, n. 124 recante «Misure urgenti connesse con la scadenza della dichiarazione di emergenza epidemiologica da COVID-19 deliberata il 31 gennaio 2020 e disciplina del rinnovo degli incarichi di direzione di organi del Sistema di informazione per la sicurezza della Repubblica».

Per far sì che ciò si concretizzi, bisogna far calare, secolarizzare come direbbe il miglior filosofo contemporaneo, due ulteriori concetti che permeano direttamente gli ambiti sociali e aziendali. Il primo è una maggiore e migliore gestione e attuazione della cosiddetta sicurezza delle e sulle informazioni e l'altra è una migliore comprensione del classico Ciclo dell'Intelligence, abile strumento aziendale per orientarsi in un mondo già troppo pieno di informazioni molteplici e tante volte inutili.

Rischio e prevenzione: la sicurezza delle e sulle informazioni

Al concetto di rischio si affianca necessariamente quello della sua gestione. A tal proposito, è importante diffondere una consapevolezza e una sensibilizzazione al tema della sicurezza delle informazioni, e in particolare per quel che riguarda l'ambito aziendale, tra il personale e il sistema Paese. Le aziende, indipendentemente dalla loro dimensione o dal settore di appartenenza, possono, anzi devono realizzare uno standard per la sicurezza delle informazioni al proprio interno, seguendo, appunto, la norma. Si tratta della certificazione ISO-27001, che descrive un metodo che le aziende devono applicare al fine di garantire uno standard elevato di sicurezza dei dati. Per ottenere una certificazione, è prioritario assicurare protezione e obblighi dei vertici della direzione, che devono attuare con successo un ISMS, Information Security Management System, ossia un sistema di gestione di sicurezza delle informazioni, e renderne chiari a tutti gli obiettivi, che saranno poi il quadro di riferimento per gli sviluppi futuri. Si passa successivamente a definire i campi di applicazione dell'ISMS, con relativa analisi dei rischi e dei punti deboli del sistema aziendale e, ovviamente, le misure da attuare in caso di incidenti,

il cosiddetto pre-audit, al quale segue il vero audit per l'ottenimento della certificazione tramite un ente indipendente.

Grazie alla certificazione ISO-27001 i processi del Sistema Paese, vedi il nostro Golden Power, un istituto legislativo di matrice britannica introdotto nel nostro ordinamento con il D.L. 15 marzo 2012 n. 21 e il Perimetro di Sicurezza Nazionale Cibernetica, istituito ai sensi dell'articolo 1, comma 1, del D.L. 21 settembre 2019, n. 105, convertito con modificazioni dalla L. 18 novembre 2019, n. 133 (in G.U. 20/11/2019, n. 272), vengono ottimizzati in quanto si riducono i tempi di registrazione degli incidenti, diminuiscono i rischi nazionali e i rischi di responsabilità. Tutto questo per una mitigazione e una collaborazione costante tra servizi di sicurezza, aziende PA e cittadini.

Il Ciclo dell'Intelligence

La consacrazione del metodo chiamato Intelligence all'interno dei Servizi segreti arriva con il cosiddetto "Ciclo dell'Intelligence" che oggi più che mai ha un rapporto diretto con la quotidianità. Si tratta di un processo che comprende cinque fasi: direction o pianificazione, collection o raccolta, processing o interpretazione, analysis o analisi, e dissemination o comunicazione.

La prima fase, ossia la pianificazione, sceglie i parametri per gli obiettivi della ricerca e i suoi requisiti, concentrandosi sull'informazione da ottenere, rispondendo alle cosiddette "5 W": Che cosa (What), Quando (When), Dove (Where), Chi (Who) e Perché (Why). Si passa, poi, alla raccolta, quindi all'acquisizione di dati grezzi o informazioni, utilizzando fonti aperte, ad esempio libri o giornali, fonti chiuse, come informazioni segrete che derivano da sorveglianza, interrogatori o operazioni segrete, e fonti tecniche, quelle elettroniche o satellitari. Raccolti i dati, è il momento dell'elaborazione, ossia della loro decodifica e interpretazione, con la conseguente valutazione della loro attendibilità, l'annotazione di quelli più rilevanti e la stima della loro utilità. Ecco che, quindi, arriva lo step chiave del Ciclo di Intelligence, ossia l'analisi. In questa quarta fase l'analista non solo riorganizza le nuove informazioni e i dati in un solo formato, ma li converte in qualcosa di significativo, il prodotto finito, che include la valutazione, l'integrazione e l'analisi dei dati disponibili. Solitamente, le tecniche messe in campo dall'analista in questa fase sono le structured analytic techniques, dette anche SATs, tecniche analitiche strutturate che aiutano a esprimere in maniera più efficace pensieri propri e risultati. Arriviamo all'ultima fase, quella della comunicazione, che deve necessariamente adottare una forma appropriata, un mezzo adatto e una struttura BLUF, ossia Bottom Line Up Front, che, in parole povere, vuol dire andare subito al sodo. Tutte le metodologie impiegate per la ricerca e l'elaborazione delle notizie sono denominate INTs, che sta per Intelligence Collection Disciplines, discipline di raccolta di Intelligence, e sono classificate come: Humint (Human Intelligence), raccolta di informazioni per mezzo di contatti interpersonali; Sigint (Signals Intelligence), raccolta di informazioni attraverso intercettazioni e analisi di segnali emessi tra persone e/o tra macchine; Geoint (Geospatial Intelligence), i dati e le immagini georeferenziati; Masint (Measurement and Signature Intelligence), la raccolta di misure metriche, angolazioni, lunghezze d'onda, rapporti temporali, modulazioni e idromagnetismo; Osint (Open Source Intelligence), le informazioni che derivano dalle fonti aperte.

Prossimo incontro
Cyber Think Tank Assintel

16 Maggio 2023

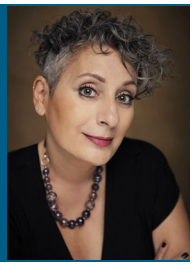
15:00

Unisciti a noi nel prossimo meeting.

Scrivi a :
segreteria@assintel.it

Lo scenario dei cyber attacchi e i principali trends

A cura di Sofia Scozzari



Il 2022 è stato l'anno peggiore in termine di evoluzione delle minacce cyber ed i relativi impatti.

In questo contesto già preoccupante, situazioni irrisolte, come la pandemia Covid-19, o altamente problematiche, come il conflitto europeo, hanno avuto forti ripercussioni anche nel mondo cyber.

Vediamo quindi come si è caratterizzato lo scenario dei cyber attacchi e quali sono stati i principali trend dell'ultimo anno.

Lo scenario globale

Da oltre 12 anni in Hackmanac ci occupiamo dell'analisi e della classificazione di cyber attacchi globali andati a buon fine e divenuti di pubblico dominio.

Questa ricerca ci consente di ottenere un'interpretazione approfondita e sempre aggiornata dell'evoluzione delle minacce informatiche e una chiara comprensione dei loro veri impatti su diverse industrie.

In questo periodo abbiamo identificato oltre 16.000 cyber attacchi, di cui 9.633 avvenuti negli ultimi 5 anni, evidenziando una chiara accelerazione nel fenomeno delle minacce cyber.

Nel 2022 abbiamo classificato la cifra record di 2.489 cyber attacchi, con una media mensile di 207 incidenti (era 171 nel 2021).

La crescita degli attacchi rispetto all'anno precedente è stata del 21% e del 60% confrontata con il 2018.

Il mese peggiore è stato marzo, dove abbiamo classificato 238 cyber attacchi, in parte certamente dovuti all'inizio del conflitto europeo.

Le motivazioni degli attacchi

Nel 2022 aumentano sostanzialmente tutte le categorie di attaccanti.

Il Cybercrime rappresenta tutt'ora la motivazione principale degli attacchi: l'82% degli incidenti è avvenuta a supporto di attività cybercriminali (in crescita del 16% rispetto all'anno precedente).

Le attività correlate a Cyber Espionage crescono del 19%, ma soprattutto aumentano in modo considerevole le azioni di Information Warfare (+110%). In entrambi i casi le cause sono da ricercare nel conflitto tutt'ora in corso, che ha determinato un aumento delle operazioni di spionaggio ed intelligence.

Per lo stesso motivo si nota un aumento anche nelle attività di Hacktivism (+320%), che impressiona ancora di più considerando che negli anni precedenti il fenomeno era quasi scomparso. Nel 2022 invece diversi gruppi di hacktivisti sono scesi in campo schierandosi per prendere le parti di entrambe le fazioni coinvolte nel conflitto Russia – Ucraina.

Le vittime

"Multiple targets", ovvero la categoria che rappresenta attacchi vittime appartenenti a differenti settori e colpite in parallelo dallo stesso attacco, torna ad essere il target principale degli incidenti nel 2022. Ciò dimostra che gli aggressori sono sempre più organizzati e motivati, in grado di condurre operazioni su scala sempre crescente al fine di massimizzare i guadagni o gli obiettivi.

Al secondo posto tra i settori più presi di mira, il settore sanitario e le entità governative, militari e di polizia (in entrambi i casi, 12% dei cyber attacchi totali).

Il settore sanitario si conferma nuovamente tra i primi target dei cyber attacchi, a riprova che l'emergenza pandemia non ancora risolta ha ancora un peso nel mondo cyber.

Menzione d'onore per i settori cresciuti maggiormente rispetto agli anni precedenti, in particolare Manufacturing che raggiunge una quota record del 5% degli attacchi totali, con una aumento del 79% rispetto al 2021.

Aumentano anche gli attacchi verso il settore News/ Multimedia (+70%), in molti casi anche per le operazioni di disinformazione causate dal conflitto europeo.

La geografia delle vittime mostra che nel 2022 le vittime in America, che storicamente rappresentavano quasi la metà del campione, diminuiscono (dal 45% degli attacchi totali nel 2021 al 38%), così come quelle in Asia e Middle East (dal 12% all'8%).

Aumentano invece gli attacchi in Europa (dal 21% al 24%), raggiungendo la soglia record di quasi un quarto degli incidenti totali classificati.

Parte di questo aumento è certamente dovuto al conflitto in corso, ma anche alle normative (GDPR in primis) che obbligano alla disclosure di incidenti informatici i cui effetti si iniziano a riflettere anche nel panorama cyber europeo.

Le tecniche di attacco

Nel 2022 il Malware resta stabile al primo posto tra le tecniche di attacco preferite, crescendo del 7% rispetto all'anno precedente e rappresentando il 36% degli attacchi totali.

All'interno di questa categoria di tecniche, il ransomware è certamente il tipo di software maligno più utilizzato (64% dei malware nel 2022).

Le "tecniche sconosciute" sono al secondo posto ed aumentano del 37% rispetto al 2021.

A seguire Phishing/Social Engineering, che cresce ulteriormente del 51% rispetto all'anno precedente e rappresenta il 12% del totale.

Lo sfruttamento delle vulnerabilità viene tutt'ora sfruttato nel 12% dei casi (era il 9% nel 2021).

Queste vulnerabilità includono sia le problematiche note, per cui cioè esistono rimedi come patch di sistema o update, che meno note, come nel caso degli zero-day, per cui non esiste nessun rimedio in quanto non conosciute dai vendor di prodotti e servizi. Queste sono certamente tra le insidie più pericolose, a maggior ragione considerando che rappresentano circa il 18% delle vulnerabilità totali classificate.

Le "tecniche multiple" rappresentano la quinta categoria di tattiche più utilizzate per effettuare attacchi informatici nel 2022, sfruttate nel 7% dei casi, un record rispetto agli anni precedenti, e cresciute del 72% rispetto al 2021. L'uso sempre più frequente di Tecniche Multiple, di norma associate a gruppi APT (Advanced Persistent Threat) indica la crescente complessità degli attacchi informatici che hanno caratterizzato l'anno.

Infine, i DDoS (Distributed Denial of Service), pur rappresentando solo il 4% degli attacchi totali, sono la categoria di tecniche che è cresciuta maggiormente nel 2022 (+258% rispetto al 2021), spesso utilizzata dai gruppi Hacktivisti per le loro rappresaglie da entrambi i lati del conflitto europeo.

Gli impatti degli attacchi

Nel 2022 l'80% dei cyber attacchi ha impatti gravi o gravissimi.

In particolare, la severity critica raggiunge la quota record del 36% degli attacchi, evidenziando un trend di crescita molto pericoloso.

Questa situazione evidenzia un concetto fondamentale nell'analisi degli attacchi informatici: l'aumento del numero di incidenti è senza dubbio un fattore significativo, ma non è l'unica variabile da considerare, soprattutto a fronte dell'impatto sempre più grave che questi attacchi dimostrano di avere.

La situazione italiana

In Italia nell'ultimo anno i cyber attacchi sono cresciuti del 169% rispetto all'anno precedente: siamo infatti passati dai 70 attacchi censiti nel 2021 a 188 nel 2022, dove gli incidenti informatici verso il nostro paese rappresentano la quota record ed impressionante del 7% del campione totale.

Considerando che il PIL italiano si attesta al 2,2% di quello mondiale, è evidente che il l'Italia sia sovra rappresentata nello scenario cyber.

Se gli incidenti verso il Belpaese sono quindi in notevole aumento, non si può dire la stessa cosa sulla complessità degli attacchi, che, come abbiamo visto in precedenza è una delle caratteristiche chiave nei trend globali.

I cyber attacchi che colpiscono il nostro Paese sono caratterizzati da una motivazione prevalentemente cybercriminale (93% del totale) e in oltre la metà dei casi (53%) si affidano all'utilizzo di Malware.

Le "tecniche multiple", che ritroviamo in corrispondenza di attacchi di particolare serietà, sono totalmente assenti dal panorama italiano.

È evidente che l'Italia deve incrementare le proprie cyber difese per mettersi nella condizione di poter contrastare i cyber crimini divenuti ormai routine.

Una considerazione che vale a maggior ragione nel momento in cui si prendono in considerazione i principali obiettivi degli attacchi italiani: al primo posto il settore governativo, militare e di polizia (20% degli attacchi), che include anche la pubblica amministrazione.

A seguire il settore manifatturiero, uno dei principali del tessuto produttivo italiano e che nel nostro Paese pare particolarmente preso di mira: qui, infatti, troviamo il 19% degli attacchi contro il 5% del campione globale. Inoltre, gli attacchi che colpiscono la manifattura italiana rappresentano il 27% degli attacchi di questa categoria, mostrando una pericolosa tendenza per questo settore.

Gli impatti degli attacchi italiani, infine, rispecchiano quelli globali: l'83% degli attacchi ha avuto effetti gravi o gravissimi e tra questi, il 37% con una severity critica.

Conclusioni

Il 2022 ha segnato un anno record per i cyber attacchi, che sono cresciuti sia in termini di numero che di frequenza, complessità e impatto.

Questo conferma una tendenza pericolosa e inequivocabile: gli attaccanti possono ancora contare sull'efficacia di malware, prodotti industrialmente a costi sempre più ridotti e in infinite varianti, su tecniche di phishing / social engineering relativamente semplici e sue vulnerabilità di varia natura, per raggiungere la maggior parte dei loro obiettivi.

D'altra parte, gli attacchi informatici diventano sempre più complessi e nel 2022 hanno subito l'influenza e in parte anche influenzato le circostanze attuali come il conflitto europeo e la crisi pandemica ancora in corso.

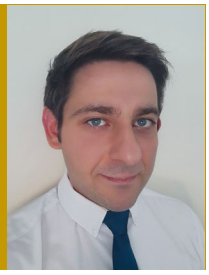
Questi eventi sono solo alcuni esempi di come i cyber attacchi stiano diventando sempre più pervasivi ed impattanti, superando i confini dell'IT e della Cyber Security, con conseguenze profonde, durature e sistemiche su ogni aspetto della società, della politica, dell'economia e della geopolitica.

Per affrontare efficacemente queste minacce, è di primaria importanza che le organizzazioni, sia pubbliche che private, riesaminino significativamente la loro postura e le strategie di Cyber Security, adattandole ai rapidi scenari di minaccia che emergono dalle analisi dei cyber attacchi.

Questo richiede l'implementazione di contromisure specifiche e mirate, che tengano conto del settore di industria, dello specifico threat model e dell'esposizione dell'azienda alle minacce informatiche.

In sintesi, il 2022 ha confermato la necessità di un approccio strategico e proattivo alla Cyber Security, che tenga conto della natura in continua evoluzione delle minacce e dell'impatto potenzialmente devastante che possono avere sulla società e sull'economia globale.

Il nuovo Standard ISO/IEC 27001:2022: quali sono i principali elementi di novità?



A cura di Riccardo Modena

Dopo un articolato processo di revisione, nello scorso mese di ottobre è stata pubblicata la nuova versione dello Standard ISO 27001.

Per chi non lo conoscesse, si tratta di un'ampia raccolta di Best Practices che le Aziende possono utilizzare per la progettazione, l'implementazione e il mantenimento di un Sistema di Gestione per la Sicurezza delle Informazioni (di seguito, SGSI) certificabile, il cui obiettivo è garantire la riservatezza, l'integrità e la disponibilità delle informazioni, dei dati personali e degli Asset correlati.

Fatta questa breve ma doverosa premessa, in questo articolo cercheremo di analizzare gli elementi di novità del nuovo Standard ISO 27001 e definire quali attività devono essere svolte per adeguarsi ai nuovi adempimenti.

Iniziamo dal titolo

Iniziamo col dire che uno dei cambiamenti più iconici dello Standard ISO 27001 riguarda il suo titolo: il nuovo nome scelto dall'International Organization for Standardization è infatti "Information Security, Cyber Security and Privacy Protection".

Un interessante cambiamento rispetto al passato, che sottolinea la portata dei temi trattati, enfatizza lo stretto legame tra discipline tra loro complementari e rende l'idea di quali elementi siano stati posti al centro durante le operazioni di revisione.

Operazioni che hanno riguardato tanto il corpo dello Standard ISO 27001 (c.d. Clausole) quanto i controlli di sicurezza (c.d. Annex A).

Le Clausole

Le Clausole, che descrivono i requisiti che le Aziende sono tenute a rispettare se vogliono essere conformi allo Standard ISO 27001:2022, hanno subito alcune variazioni.

Quelle di maggiore rilevanza riguardano:

- la clausola "4.4 - Information security management system", che nella sua nuova formulazione pone al centro i processi aziendali e le loro interazioni, la cui gestione rappresenta una condizione sine qua non per il corretto funzionamento del SGSI;
- la clausola "6.1.3 - Information security risk treatment", che introduce alcune novità relative allo Statement of Applicability, il quale potrà includere

controlli diversi da quelli presenti nell'Annex A, a patto che se ne giustifichi il motivo d'inclusione;

• la nuova clausola "6.3 - Planning of changes", che sottolinea l'importanza della gestione dei cambiamenti (c.d. Change Management) e ne richiede la pianificazione, specie se questi hanno impatti sul SGSI;

• la nuova clausola "8.1 - Operational planning and control", che richiede alle Aziende di controllare con la massima attenzione i prodotti e i servizi forniti esternamente, specie se rilevanti per il SGSI.

Le restanti modifiche alle Clausole aggiungono poco valore allo Standard ISO 27001, per cui è meglio spostare la nostra attenzione sui nuovi controlli di sicurezza.

L'Annex A

I cambiamenti più rilevanti riguardano sicuramente l'Annex A, ovvero quella sezione dello Standard ISO 27001 che integra le Clausole con una serie controlli di sicurezza a cui le Aziende possono fare riferimento nell'ambito dei propri processi di gestione del rischio.

Una revisione generale

Nella sua precedente versione, l'Annex A era composto da n. 114 controlli di sicurezza, suddivisi in n. 14 domini, che indirizzavano i diversi aspetti della sicurezza delle informazioni (es. politiche, organizzazione interna, gestione degli Asset e degli accessi logici, sicurezza fisica, ecc.).

Queste categorie sono state abbandonate a favore di n. 4 nuovi raggruppamenti:

- People controls;
- Physical controls;
- Technological controls;
- Organizational controls

Anche i controlli di sicurezza che compongono l'Annex A sono stati rivisti e grazie ad alcuni accorpamenti, passano da n. 114 a n. 93.

È bene precisare che queste modifiche attengono più alla forma che alla sostanza: certamente il numero dei controlli di sicurezza è inferiore rispetto al passato, ma i loro contenuti risultano pressoché invariati (se non addirittura arricchiti).

I nuovi controlli di sicurezza

L'aspetto sicuramente più dirompente della nuova versione dello Standard ISO 27001 è l'introduzione di n. 11 nuovi controlli di sicurezza, che focalizzano diversi temi di assoluto interesse. Nello specifico:

• Il controllo "A.5.7 - Threat intelligence" richiede l'adozione di processi e di strumenti che consentano l'individuazione e la prevenzione delle minacce informatiche emergenti. Lo svolgimento di analisi tecniche (es. Vulnerability Scan, Penetration Test, ecc.) è sicuramente importante ma lo è anche il monitoraggio delle principali fonti informative in tema (es. OSINT, Bulletins, ecc.);

• Il controllo "A.5.23 Information security for use of Cloud services" arricchisce le Best Practices già definite in tema di governance dei rapporti di fornitura focalizzandole sulla sicurezza dei servizi Cloud. In questo caso è richiesto, in sintesi:

  - l'adozione di processi per la selezione o il monitoraggio dei Provider;
  - la definizione di una politica relativa all'utilizzo dei servizi Cloud;
  - la gestione dei rischi associati a tali tecnologie;
  - la stipula di contratti che definiscano le responsabilità delle parti.

• Il controllo "A.5.30 - ICT readiness for business continuity" affronta il tema della continuità operativa, che deve essere pianificata e monitorata al fine di assicurare che le strategie definite dalle Aziende siano supportate dall'infrastruttura esistente. L'effettiva applicazione di questo controllo non può prescindere dall'analisi preventiva dei processi critici per il Business e dei relativi impatti in caso di interruzione degli stessi (c.d. Business Impact Analysis);

• Il controllo "A.7.4 - Physical security monitoring" richiede l'adozione di soluzioni per il controllo e il monitoraggio delle sedi, degli uffici e dei locali tecnologici (es. videosorveglianza, sistemi

antintrusione, allarmi, ecc.).

• Il controllo "A.8.9 - Configuration management" introduce il delicato tema della configurazione sicura dei sistemi e affronta il tema dell'hardening. L'obiettivo di fondo è spingere le Aziende ad adottare un sistema di gestione delle configurazioni, supportato da strumenti commisurati alle esigenze del Business (es. Template, Configuration Management Database, ecc.).

• Il controllo "A.8.10 - Information deletion" richiama il concetto della cancellazione dei dati personali e lo estende all'intero patrimonio informativo dell'Azienda. Il tema principale è la restituzione e/o la cancellazione dei contenuti relativi ai Clienti (es. in seguito alla conclusione dei rapporti contrattuali), che le Aziende devono indirizzare definendo chiaramente responsabilità, procedure o modalità operative.

• Il controllo "A.8.11 - Data masking" ci parla di anonimizzazione, pseudonimizzazione e mascheramento: tre tecniche che devono essere impiegate in funzione della criticità delle attività svolte.

• Il controllo "A.8.12 - Data leakage prevention" richiede l'adozione di processi e di strumenti che consentano di identificare, monitorare e proteggere le informazioni e i dati personali al fine di prevenirne l'uso illecito o la trasmissione non autorizzata. Questo obiettivo può essere raggiunto sia attraverso il monitoraggio delle reti aziendali (es. attraverso i Firewall di ultima generazione che includono diverse funzionalità in grado di contrastare l'esfiltrazione di contenuti) sia mediante iniziative, che vanno da una corretta gestione delle utenze e dei privilegi a misure di più basso livello, come ad esempio il blocco delle porte USB o l'inibizione dei servizi di condivisione non autorizzati (es. piattaforme Web, ecc.).

• Il controllo "A.8.16 - Monitoring activities", già presente in alcuni controlli del vecchio Standard ISO 27001, richiede di porre attenzione al monitoraggio di reti, sistemi, dispositivi e applicazioni al fine di rilevare eventuali anomalie.

• Il controllo "A.8.23 - Web filtering" sottolinea l'importanza di presidiare una delle attività più pericolose e in grado di esporre gli utenti ai rischi della Cyber-Security: la navigazione Web. Il suggerimento è quello di adottare soluzioni di Web Filtering, in modo da ridurre il rischio che il personale acceda a siti Web malevoli.

• Infine, il controllo "A.8.28 - Secure coding" richiede la definizione di politiche e procedure per lo sviluppo sicuro del software. Non serve reinventare la ruota ma iniziare ad integrare nei propri processi una serie di buone pratiche, come:

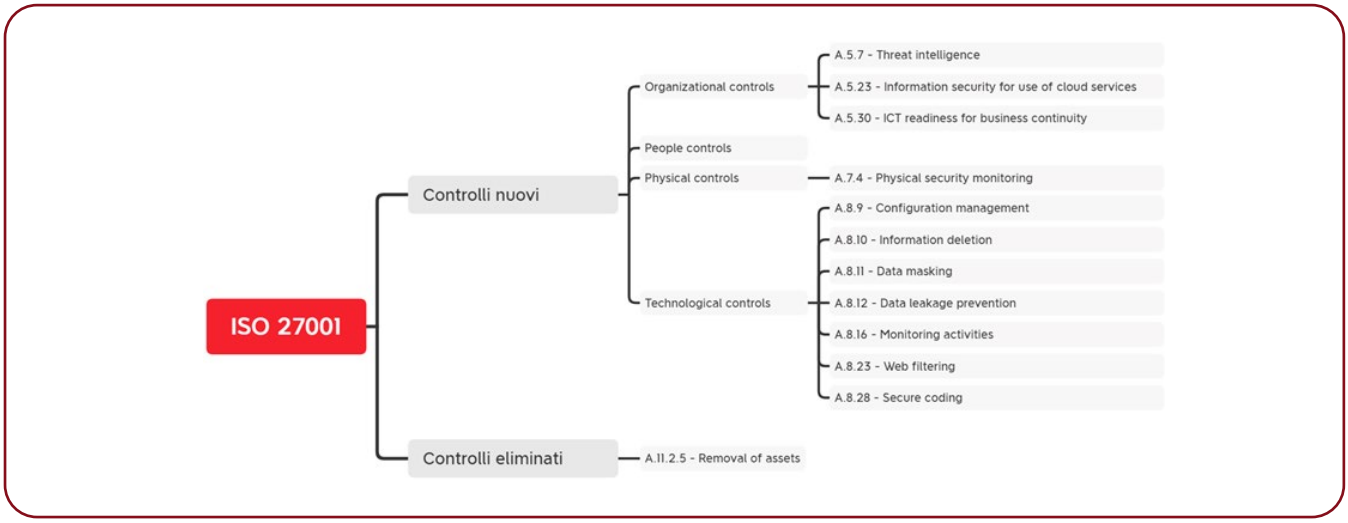
  ◦ Le line guida di OWASP per la sicurezza delle applicazioni Web e delle API.

  ◦ I suggerimenti di CWE per la rimozione delle principali vulnerabilità software.

  ◦ I Coding Standard emessi dal CERT, da AGID o dal NIST (es. NIST.SP.800-218).

Le attività di adeguamento

Ora che abbiamo analizzato i principali cambiamenti introdotti dal nuovo Standard ISO 27001 non ci resta che capire come gestirli, soprattutto in ottica di migrazione del proprio SGSI. Di seguito, alcuni suggerimenti:



• Chi ha tempo non aspetti tempo - Occorre avviare e concludere il processo di migrazione nei giusti tempi, in modo da evitare che le certificazioni si concentrino in prossimità della data di scadenza, mettendo in difficoltà gli Enti di Certificazione;

• Pianificate i cambiamenti - Le cose da fare possono essere molte, per cui è meglio procedere con ordine:

  ◦ Adeguare i processi, le politiche e le procedure.

  ◦ Adottare nuove procedure o strumenti per indirizzare i controlli aggiuntivi.

  ◦ Aggiornare le Checklist di Audit e le metodologie di Risk Assessment.

  ◦ Rivedere lo Statement Of Applicability.

  ◦ Definire indicatori per monitorare i nuovi controlli e processi.

  ◦ Svolgere la necessaria formazione del personale.

• Prestate attenzione nell'aggiornamento delle politiche. Sulla base della mia esperienza personale, consiglio di procedere per Step:

  ◦ Riordinare i contenuti secondo i nuovi domini dello Standard ISO 27001.

  ◦ Verificare se le politiche necessitano di integrazioni, utilizzando come riferimento lo Standard ISO 27002.

  ◦ Integrare le politiche dando spazio ai nuovi n. 11 controlli.

• Fate attenzione ai Risk Assessment: uno degli aspetti fondamentali di qualsiasi analisi dei rischi è la possibilità di poterne comparare i risultati anno su anno. Il consiglio è quello di non modificare di punto in bianco la propria metodologia di Risk Assessment ma effettuare - se possibile - un passaggio intermedio, in modo da produrre risultati coerenti e comparabili nel tempo;

• Per ciò che riguarda l'aggiornamento dello Statement of Applicability ho un unico suggerimento: fino a quando non deciderete di rivedere integralmente la vostra impostazione (riprendendo la struttura del nuovo Standard ISO 27001), i nuovi controlli possono essere considerati come aggiuntivi o integrativi.

Occhio alle date

Infine, se state affrontando una prima certificazione o una migrazione alla nuova versione dello Standard ISO 27001, è bene che prestiate attenzione a queste date:

• Il 31 Ottobre 2022 è l'ultimo giorno del mese di pubblicazione del nuovo Standard ISO 27001: da questo momento in poi, tutte le Aziende interessate potranno richiedere la certificazione o la migrazione alla versione più recente della norma;

• Il 31 ottobre 2023 è l'ultima data utile per avviare una prima certificazione secondo il vecchio Standard ISO 27001:2013; da questo momento in poi gli Enti di Certificazione avvieranno solo certificazioni basate sulla nuova norma;

• Il 31 ottobre 2025 è la data entro la quale tutti certificati dovranno essere migrati alla nuova versione dello Standard ISO 27001. ATTENZIONE: l'intero iter di migrazione, incluso l'Audit dell'Ente di Certificazione, deve essere completato entro questa data (non solamente avviato).

La sicurezza informatica nel settore dell'avionica

A cura di Raoul Chiesa

1. SCENARIO

Fornitori di hardware e software per il mercato Aero*, vendono piattaforme, applicazioni e sistemi che, in genere, sono estremamente insicuri, dal punto di vista della sicurezza delle informazioni, della cybersecurity, della privacy. Per essere più gentili, potremmo dire che almeno gli aspetti della sicurezza delle informazioni non sono in cima alla loro lista. Gli operatori dell'industria dei trasporti non hanno (ancora una volta: tipicamente, ma con alcune aspettative difficili da trovare e molto rare) una visione corretta e una comprensione sufficiente delle nuove sfide legate alla sicurezza ICT.

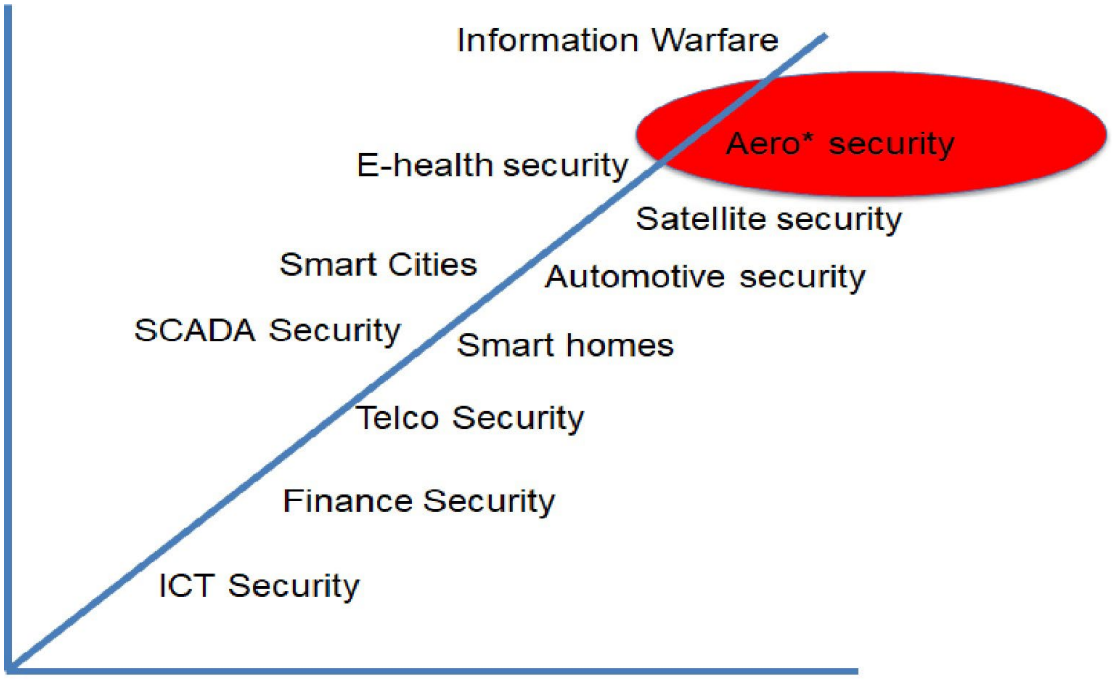
2. In generale, il grafico seguente mostra la cosiddetta Esposizione a minacce sconosciute in base al "contesto puntuale" di diversi settori industriali, tra i quali possiamo trovare anche quello dell'Avionica.

Il problema chiave

Molto tempo fa, intorno al 2005, sono stato ingaggiato, insieme al mio team tecnico di Cybersecurity, da un aeroporto internazionale europeo. L'obiettivo era quello di eseguire un "test di penetrazione" (simulando un vero attacco informatico) contro l'intera infrastruttura ICT dell'aeroporto.

Stavo parlando con i tecnici del cliente e in qualche modo mi hanno aperto gli occhi.

Il tipo mi ha detto: "Noi siamo solo l'Internet Service Provider (ISP) dell'aeroporto. Noi (ri)vendiamo "servizi", come il "trasporto dati": pensate a SITA, ai POS dei negozi Duty Free, alle interconnessioni con le forze dell'ordine (Dogana, Immigrazione, ecc.), e così via. Anche "cose semplici" come il "Free Wifi" che si trova in tutti gli aeroporti del mondo!



3. Hacker e sicurezza degli aerei

Nonostante la fiducia nelle industrie aeronautiche e avioniche, la comunità degli hacker etici ha "scoperto" la mancanza di sicurezza informatica in queste industrie molto tempo fa!

Tra il 2006 e il 2014 molti hacker etici e ricercatori di sicurezza, come Hugo Teso (Germania), Renderman (Canada), Ruben Santamarta (Spagna) e il sottoscritto (Italia), solo per citarne alcuni, hanno iniziato a "dare la caccia" alle vulnerabilità in questo specifico settore industriale.

Presentazioni pubbliche come "Hackers + Airplanes: no good can come of this" portano titoli che si spiegano da soli!

4. Caso di studio: Errori nelle RFQ di Penetration Test

Molto spesso, quando abbiamo avuto a che fare con clienti dell'industria avionica per progetti di Penetration Test, abbiamo riscontrato molteplici errori nelle Richieste di Offerta:

- Le aree ICT chiave (asset dell'infrastruttura di rete) da testare mancavano nello Scope of Work (ToE: Target of Evaluation).
- I clienti non chiedevano una metodologia specifica e standard a livello mondiale da utilizzare nei Penetration Test.
- Non c'è sufficiente conoscenza dei problemi di sicurezza ICT.
- Mentalità sbagliata e mancanza di consapevolezza della Cybersecurity e della contestualizzazione dei Cyberattacchi.
- Mancanza di budget: la maggior parte dei clienti diceva "Vogliamo testare tutto", mentre il budget a disposizione consentiva solo un "piccolo" test.
- 100% concentrato solo su ISO/IEC: tutti noi conosciamo le ISO/IEC (27001, 27005, ecc. ecc.: c'è una ISO per ogni settore!). La conformità a una ISO/IEC consente all'azienda di essere "etichettata" con un timbro ufficiale dell'ISO, aiutando le Procedure, le Politiche, il Ruolo delle Risorse Umane, ecc.... D'altra parte, quando si tratta di ISO/IEC relative alla sicurezza delle informazioni, tali conformità non rappresentano una reale sicurezza ICT: una valutazione di sicurezza ISO/IEC è solo una valutazione teorica (interviste, documenti, procedure, ecc.), non un test di sicurezza sul campo.

La maggior parte degli errori sopra descritti sono dovuti a un approccio totalmente sbagliato alla sicurezza delle informazioni: il cosiddetto "paradigma CIA".

CIA sta per i tre pilastri della sicurezza informatica.

Per essere "sicuro", un sistema informatico deve conservare i dati (informazioni) che memorizza ed elabora tenendo conto di tre paradigmi:

- Riservatezza (R) dei dati;
- Integrità (I) dei dati;
- Disponibilità (D) dei dati.

Ora, si capisce subito come questo approccio non si adatti a diversi settori, come quello dell'avionica o quello dei servizi di pubblica utilità (elettricità, acqua, ecc.), solo per citarne uno meno complicato.

Infatti, quando si tratta di servizi di pubblica utilità troviamo un approccio opposto: AIC.

I dati (la vostra bolletta elettrica) devono essere prima di tutto Disponibili (D), poi come secondo Integro (I) e solo come ultima importanza e priorità, Riservati (R).

Il significato complessivo è che se non c'è una bolletta dell'elettricità, non c'è bisogno di occuparsi né della sua (I) né della sua (R).

Questo esempio tratto dalla vita reale spiega perché gli esperti di Cybersecurity si trovano spesso in difficoltà quando si occupano di questioni di sicurezza delle informazioni insieme a esperti di mercati diversi, come quello degli SCADA e dell'automazione industriale - e il settore dei trasporti rientra in questa categoria. Si tratta di mentalità diverse, guidate da priorità diverse.

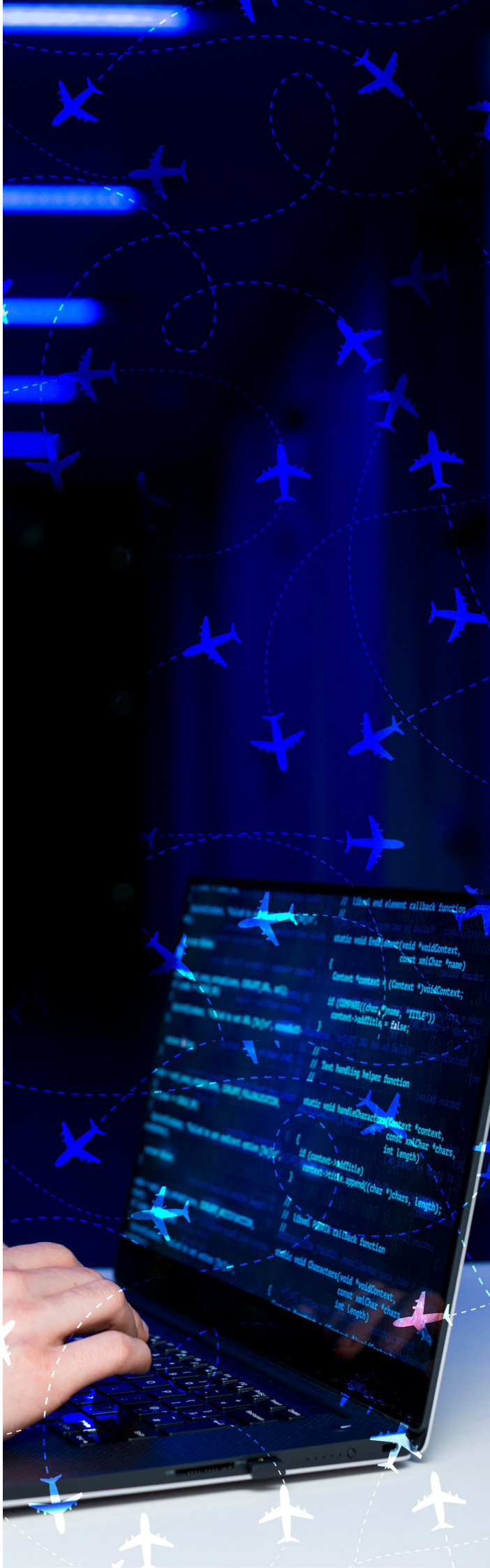
Cosa potete fare VOI?

La cybersecurity nell'avionica è qualcosa di rilevante per tutti noi: operatori di mercato, utenti finali, responsabili politici, legali, manutentori, integratori e cittadini.

Durante l'ultimo WAS 2023 in Svizzera (Winter Avionics Summit, Vivey, marzo 2023), e grazie alla lungimiranza di Gina Whitehead Girona che ha creato il WAS, io e la mia collega Serena Giugno abbiamo tenuto una conferenza della durata di 3 ore".

È stato molto utile per tutti i partecipanti, provenienti da diversi ambienti del settore avionico: hanno imparato cosa può accadere, perché, ma soprattutto cosa può fare l'azienda violata in modo proattivo, per evitare che tali incidenti si verifichino.

Ecco perché di seguito fornisco a tutti i lettori di questa rivista una panoramica di alto livello delle azioni chiave da



eseguire all'interno della vostra organizzazione.

a) Consapevolezza della sicurezza

"Non c'è rimedio alla stupidità umana": una frase molto forte che riprende uno dei problemi principali quando si tratta di Cybersecurity... il fattore umano, chiamato anche "l'anello più debole della catena".

Ci sarà sempre un utente, un dipendente, un consulente, chiunque... che cliccherà su un link dannoso, piuttosto che inserirà una chiave USB nel posto sbagliato, e così via.

Per "rimediare" a questo problema ed evitare tali minacce, è necessario sensibilizzare l'organizzazione alla sicurezza informatica.

Ciò avviene in diversi modi, come ad esempio sensibilizzazione a distanza o in loco da parte di esperti di sicurezza informatica, videoclip e materiale intranet (come le diapositive) in modo che i dipendenti siano costretti a guardarli, e la politica di sicurezza informatica dell'azienda, che fa rispettare le linee guida di "buona condotta".

b) OSINT - Open Source Intelligence

Indipendentemente dal settore, ogni organizzazione dovrebbe avere installato e "pronto all'uso" una piattaforma OSINT, piuttosto che un fornitore esterno di OSINT, per essere informata in tempo reale su ogni informazione pubblica relativa al proprio settore, ai propri fornitori e alla catena di fornitura (come richiesto dal regolamento europeo GDPR), ecc.

c) Dark Web e Deep Web

Proprio come per l'OSINT, lo stesso approccio logico dovrebbe essere eseguito su tutti i dati appartenenti alla vostra organizzazione che sono già stati "rubati" e possono essere trovati "in vendita" sul Dark Web e sul Deep Web.

Nel corso del mio workshop abbiamo controllato molte aziende (domini, siti web, indirizzi e-mail), lasciando tutti i delegati a bocca aperta.

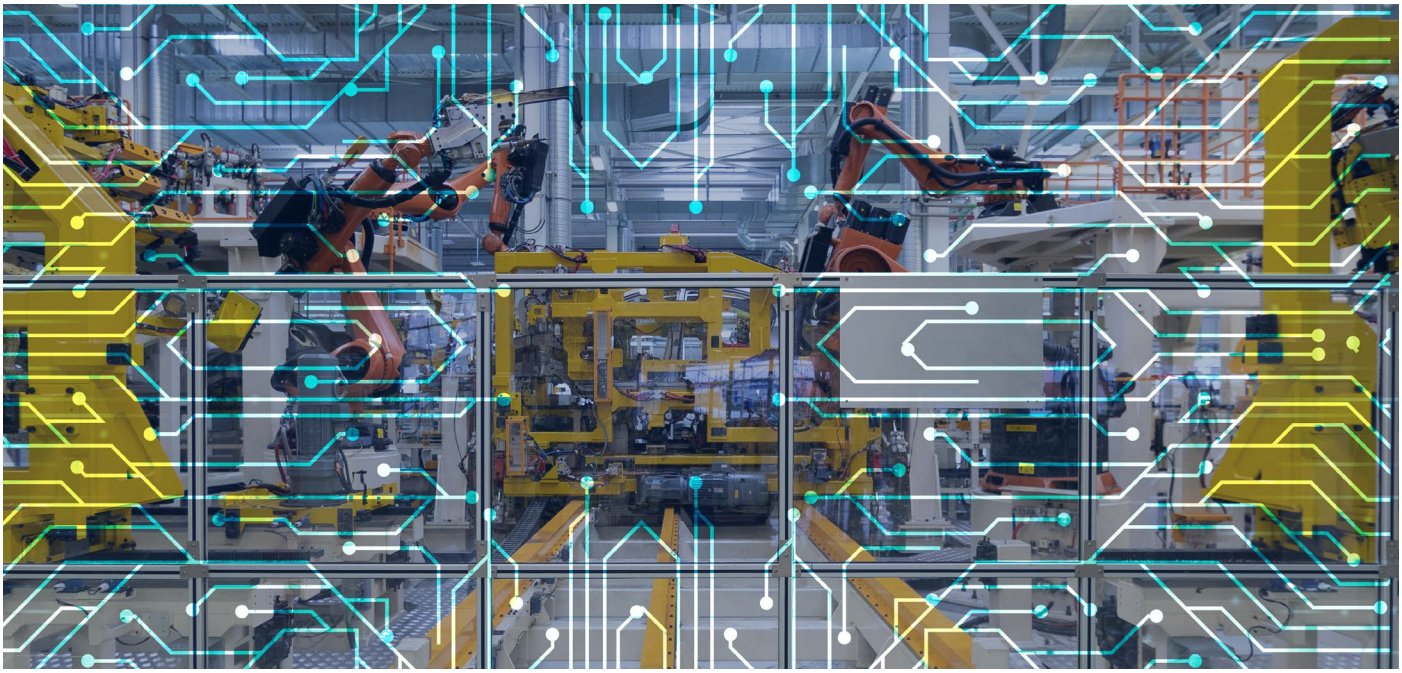
Anche in questo caso, un'organizzazione può acquistare una soluzione di terze parti e utilizzarla in proprio, anziché affidare il lavoro a società esterne di consulenza in materia di Cybersecurity, allertando così l'organizzazione quando viene scoperto qualcosa di "cattivo, illegale e pericoloso".

d) Valutazioni di sicurezza

Una valutazione di (Cyber)Security è molto simile al nostro check-up personale, quello che ognuno di noi (dovrebbe) fare regolarmente ogni anno: un giorno di Day-Hospital con tutti gli esami medici, le analisi, ecc.

La stessa cosa accade alla vostra organizzazione, quando si esegue una serie di "controlli" sulla vostra "Postura di Cybersecurity".

Questo può essere effettuato con due diversi "livelli"



di profondità, ottenendo così un risultato molto più dettagliato: un Vulnerability Assessment o un Penetration Test.

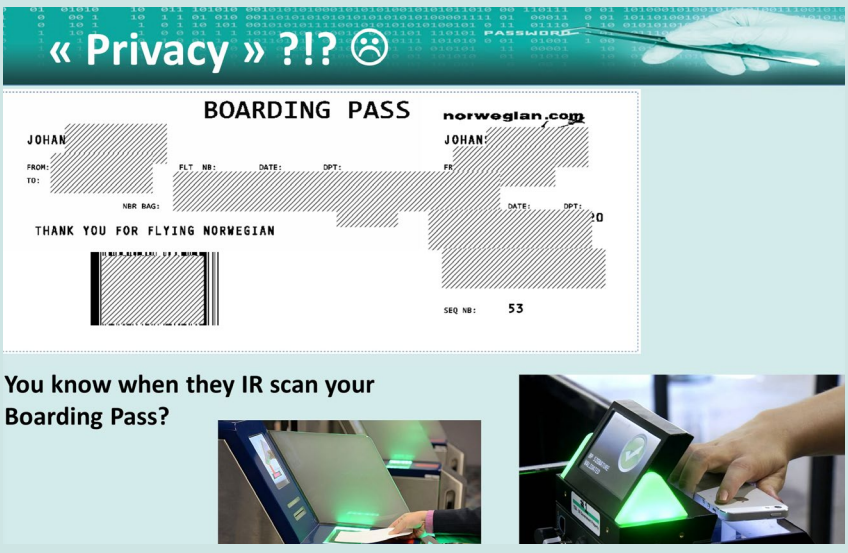
Il mio consiglio è di optare per un Penetration Test: questo replicherà le azioni esatte di diversi aggressori ("hacker", "attori della criminalità informatica", "attacchi sponsorizzati da uno Stato", "terroristi informatici", ecc.)

Caso di studio: Aeroporti e Penetration Test

Per far capire ai lettori non tecnici i benefici e i risultati di un rapporto di Penetration Test, ecco un piccolo "allegato" a questo articolo.

Era il 2005 e, come ho scritto all'inizio, ero stato ingaggiato per conto di una delle mie società di Cybersecurity da un aeroporto internazionale europeo. Abbiamo eseguito sia "attacchi IT e ICT", sia "attacchi di intrusione fisica", sia "attacchi di ingegneria sociale".

Di seguito pubblico alcune evidenze (sanificate) del rapporto, con la speranza che questo possa aiutare altre aziende che gestiscono i servizi aeroportuali in altri paesi del mondo.



Cyber Think Tank Assintel

ASSINTEL CYBER SECURITY

Cyber Think Tank Assintel

PARTECIPA ANCHE TU!

Scrivi a: segreteria@assintel.it

ASSINTEL
ASSOCIAZIONE NAZIONALE IMPRESE ICT

CYBER MAGAZINE

Anno4 / Numero 6
2023

ASSINTEL CYBER SECURITY

ASSINTEL
ASSOCIAZIONE NAZIONALE
IMPRESE ICT

Contattaci

info@assintel.it

www.assintel.it