AI, CYBERSECURITY E NIS II: ESPERIENZE E SCENARI

ore 9:40 – 11:25 – OPEN ARENA

Sommario

Introduzione

L'incontro di apertura della seconda edizione di **Orizzonti Digitali** ha visto la partecipazione di illustri relatori, tra cui **Gabriele Picchi**, **Alessandro Calabrese**, **Mario Finetti**, **Maurizio Genna** e **Giuseppe Dongu**. Questi esperti, coordinati da **Mariano Gattafoni**, hanno condiviso le loro esperienze e conoscenze sui temi cruciali della Cyber sicurezza e della NIS II, affrontati da diverse angolature. L'evento ha rappresentato un'importante occasione per approfondire lo stato

dell'arte e le prospettive future della Cyber, anche alla luce del ruolo che avrà l'Intelligenza Artificiale, sia in termini di minacce che di difese.

I temi chiave del panel

1. **L'importanza del controllo della catena di fornitura**
2. **Direttiva NIS II e normative italiane ed europee**
3. **L'intelligenza artificiale e la continuità delle organizzazioni**
4. **Chiudere la stalla dopo che i buoi sono scappati**
5. **La sicurezza del software**
6. **Intelligenza artificiale e cyber**
7. **L'importanza delle certificazioni, in particolare della ISO 27001**
8. **L'autorefenzialità non basta**
9. **Intelligenza artificiale e norme tecniche**
10. **La difficoltà di scegliere le priorità**
11. **Competenze di cybersecurity nelle PMI**
12. **Il Cyber Resilience Act**

Gabriele Picchi

L'importanza del controllo della catena di fornitura

Gabriele Picchi ha iniziato il suo intervento richiamando quanto accaduto il 13 agosto 2024, quando un importante quotidiano nazionale, e tre testate regionali ad esso collegate, non sono usciti né in edicola né in versione digitale. La responsabilità è stata attribuita da parte del quotidiano al fornitore primario di telecomunicazioni e datacenter del gruppo.

Si tratta di un evento – ha sottolineato Picchi - che ha una doppia veste dal punto di vista della lettura di quello che è accaduto, perché da un lato impatta il **controllo della catena di fornitura** - uno dei temi più importanti per il contesto cybersecurity e che la direttiva NIS identifica tra le proprie iniziative – e dall'altro **coinvolge** una realtà, **il fornitore di servizi di telecomunicazione** e datacenter, che è una di quelle strutture primarie che sono necessariamente chiamate a rispondere alla direttiva NIS II. È perciò indubbiamente un tema di cybersecurity forte, anche se, al momento, la risposta del fornitore ufficiale ha ricondotto l'inconveniente ad un danno ai sistemi di condizionamento del datacenter.

Se si ragiona da addetti ai lavori, non ci si può non domandare come la proprietà del giornale non abbia mai preso in considerazione degli scenari di impatto e di crisi che avrebbero potuto portare a questo tipo di evento e come un fornitore primario non fosse mai stato sottoposto ad alcune valutazioni, ad alcuni test di *continuity* o di *disaster recovery*, anche congiunti.

Questo caso può diventare un caso scuola, perché è un esempio di applicazione pura delle condizioni di direttiva NIS II e di criticità di cybersecurity.

Picchi ha suggerito di provare ad immaginare se, anziché la mancata presenza di un quotidiano in edicola, ci fosse stata l'impossibilità ad accedere ai servizi sanitari, come è accaduto a SYNLAB pochi mesi fa, che ha letteralmente bloccato tutti i centri e reso impossibile la diagnostica per numerose settimane.

Direttiva NIS II e normative italiane ed europee

Picchi ha affermato che la direttiva NIS II e le tematiche di cybersecurity devono essere prese in considerazione sotto due profili: quello della compliance e quello del modello a cui ispirarsi. Il primo aspetto riguarda la risposta agli obblighi che i soggetti coinvolti sono chiamati ad assolvere. Il secondo concerne l'opportunità, anche per chi non è soggetto alla direttiva NIS II, di prendere in considerazione tutti i requisiti e tutti i criteri che da questa vengono messi in evidenza, perché farli propri indubbiamente costituisce una base omogenea di criteri di cybersecurity da affrontare.

Picchi ha parlato dell'importanza di controllare ad alto livello la catena di fornitura, la governance e la valutazione di rischio. La NIS II implica infatti la *governance* e la valutazione di rischio ad alto livello, a partire dai manager, ed a prendere atto di una vera e propria *accountability*, perché tra le sanzioni che prevede c'è anche quella di sospendere coloro che hanno ruoli gestionali, se a fronte di eventi di cybersecurity si dimostra che questi soggetti non hanno fatto tutto quello che avrebbero dovuto fare per la valutazione dei loro rischi e delle loro terze parti, soprattutto nell'ambito della *supply chain*. Ha menzionato che la direttiva NIS II impatterà tra le 25 mila e le 35 mila organizzazioni in Italia, che dovranno essere sottoposte ad attività di vigilanza e controllo. Ha fatto un parallelo rispetto alle tematiche critiche che possono riguardare banche, sistemi di trasporto, logistica, utility di qualunque tipo, e ha sottolineato che il contesto cybersecurity è un contesto che le organizzazioni devono iniziare a prendere sul serio.

La NIS II è ampissima, ha aggiunto Picchi, e può riguardare l'ambito alimentare, chimico, le utility di qualunque tipo - acqua, rifiuti - e poi impatta in realtà nel mondo IT, nel mondo digitale che fornisce servizi cloud, nei servizi di telecomunicazione, servizi business to business e altri.

C'è l'aspetto dimensionale che viene preso in considerazione, ma se l'azienda eroga un servizio critico, indipendentemente dalla dimensione, è tenuta ad ottemperare a quello che la direttiva chiede. Ci sono alcuni settori industriali del Paese in cui ancora queste tematiche non sono considerate primarie, ma in realtà non esiste un settore, indipendentemente da quelli previsti dalla direttiva, che non debba considerare la propria situazione in termini di cybersecurity.

L'intelligenza artificiale e la continuità delle organizzazioni

Picchi ha poi parlato dell'intelligenza artificiale e di come possa supportare e potenziare gli strumenti utilizzati per individuare problematiche di cybersecurity in maniera preventiva, proattiva e predittiva, quali i *Security Operation Center*, tutti gli strumenti evoluti di EDR, XDR e così via.

Ha anche discusso il tema della continuità delle organizzazioni, sottolineando che la *Business Continuity* non si esaurisce nel mettere in piedi dei *backup* ed eseguire dei test periodici, ma richiede per le organizzazioni vere e proprie strategie che toccano strutture, infrastrutture IT, terze parti, persone, competenze chiave che devono dimostrare che l'organizzazione è in grado di rispondere a casistiche e ad eventi di un certo tipo.

Ha aggiunto che deve diventare normale eseguire periodicamente delle simulazioni di impatto *ransomware* all'interno di qualunque organizzazione.

C'è un'"ipertrofia normativa" - direttiva CER, NIS II, GDPR, Digital Service Act eccetera- che va semplificata, ha aggiunto.

Le aziende la devono semplificare, devono prendere in considerazione gli aspetti più rilevanti affidandosi agli standard. Occorre lavorare e ragionare sugli standard, standard ISO, standard NIST e altri standard che esistono sul mercato, perché la complessità può essere razionalizzata seguendo gli standard. Un esempio banale, certificarsi, o mettere comunque in piedi un modello organizzativo basato sulla ISO 27001 che si occupa della sicurezza delle informazioni, dà una base solida per affrontare la direttiva NIS II, la CER etc.

Ha quindi concluso l'intervento richiamando la parola d'ordine che ci deve essere per tutti, imprese, colleghi, addetti ai lavori: concretezza.

Bisogna essere pragmatici, ci sono moltissime cose da fare, moltissime attività che devono essere scaricate a terra. Quindi – ha concluso Picchi- concretezza per le imprese: intercettare subito la problematica, capire qual è il tema, capire qual è l'impatto, e capire se ci sono molteplici impatti dal punto di vista della cybersecurity.

Giuseppe Dongu

Chiudere la stalla dopo che i buoi sono scappati

Giuseppe Dongu - che si occupa di soluzioni per la protezione e per la simulazione di attacchi- ha sostenuto che c'è una consapevolezza molto bassa sugli effetti causati da un possibile incidente. E si tratta, ha aggiunto, di una consapevolezza che nasce sempre dopo gli incidenti, almeno a giudicare dall'esperienza maturata negli ultimi anni.

Dongu ha evidenziato che gli incidenti di cybersecurity possono avere conseguenze gravi, tra cui l'attenzione negativa dei media, il blocco della produzione e la perdita di reputazione. L'azienda – ha proseguito – a seguito di un incidente vive spesso una situazione che è assolutamente devastante.

Quando si interviene, la prima cosa che si può fare è constatare lo stato di profonda preoccupazione in cui tipicamente gli imprenditori, o comunque le persone che lavorano in azienda, si trovano, perché si rendono conto di essere completamente bloccati e non hanno la più pallida idea di cosa devono fare per poter ripartire. Tipicamente, inoltre, questi incidenti avvengono nei periodi di festa, nei fine settimana o a ridosso delle vacanze.

Qualche anno fa, quando vi era una totale mancanza di consapevolezza, ha evidenziato Dongu - ci veniva richiesto di ripartire il lunedì, perché le imprese non si rendevano conto di quanto fosse difficile gestire la situazione.

La bassa consapevolezza aziendale fa sì che gran parte degli investimenti in cybersecurity e delle azioni intraprese in termini di governance - un *incident response plan* o la simulazione di incidenti per gli attacchi *ransomware* - avvengano dopo l'incidente. Da quel momento in avanti l'azienda è

infatti più consapevole di cosa significhi essere attaccata e quindi ha un'idea più chiara di cosa fare per prevenire un secondo incidente.

La sicurezza del software

In pochi pensano realmente di poter essere vittima prima o poi di un attacco. Il punto fondamentale – ha spiegato Dongu - è che la catena di sicurezza è tanto forte quanto è forte il punto più debole. È il punto più debole che determina la forza totale di resistenza delle misure di sicurezza.

In merito all'*Open Web Application Security Project*, Dongu ha dichiarato di avere una visione non troppo positiva. Capita spesso di vedere aziende produttrici di software che considerano la sicurezza una *feature* aggiuntiva, quindi non la base, non le fondamenta su cui dovrebbe basarsi tutto lo sviluppo, ma qualcosa che non è data per scontata. È un approccio folle, perché le vulnerabilità sulle applicazioni sono i punti attraverso i quali si viene attaccati, e quindi affidarsi a un software che è stato scritto senza aver messo la sicurezza come cardine dello sviluppo significa aver fatto partire un *countdown* e prima o poi ci sarà un cybercriminale che volutamente, o facendo pesca a strascico, troverà quella vulnerabilità e farà di tutto per sfruttarla in modo tale da poter dar luogo alle successive estorsioni.

La modellazione delle minacce dovrebbe essere il punto zero della parte di design e sviluppo del software.

Quando capita, e capita spessissimo, di trovare vulnerabilità nei software, generalmente si fa partire un *responsible vulnerability disclosure* per aiutare il *vendor* a risolvere il problema. Nel 60% dei casi, il *vendor* collabora; nel 40% diffida dal pubblicare dettagli sulla vulnerabilità, e molto spesso si tratta di *vendor* italiani. Questo dimostra – ha proseguito Dongu - che c'è un problema culturale che va risolto.

Intelligenza artificiale e cyber

In merito alla NIS II, l'intelligenza artificiale – ha detto - va vista come un grande ausilio per il monitoraggio e la valutazione di grandi moli di dati, da cui poter ottenere delle dashboard che permettano di prendere delle decisioni e fare delle valutazioni.

L'AI sta entrando in tutto ciò che è il mondo dei *security operations center* e dei SOAR, ha spiegato.

Ci sono altri due aspetti su cui riflettere. Il primo riguarda gli attaccanti. Gli attaccanti stanno iniziando a valutare e ad utilizzare strumenti di intelligenza artificiale per la produzione di malware e per cercare di nascondere le tracce di quella che si chiama l'*attribution*, cioè tentano di nascondere da chi sia effettivamente stato prodotto quel malware. Il secondo concerne il fatto che gli stessi strumenti di intelligenza artificiale possono avere delle vulnerabilità, tanto è vero che OWASP ha pubblicato due progetti nuovi, uno orientato al machine learning e l'altro orientato a quelle che sono le intelligenze generative, evidenziando i 10 rischi per ognuna di queste due tecnologie, ha concluso Dongu.

Maurizio Genna

L'importanza delle certificazioni, in particolare della ISO 27001

Relativamente alle certificazioni, uno spartiacque importante, che ha dato una spinta alla certificazione, soprattutto 27001, è stato il Regolamento europeo privacy che ha favorito, anche grazie alle possibili sanzioni, un approccio diverso da parte dei responsabili IT.

In precedenza, - ha proseguito Genna - c'era da parte loro una chiusura perché non volevano che altri entrassero nel merito delle azioni da loro intraprese. Con il DGPR, capendo che la responsabilità di incidenti di information security e cybersecurity sarebbe caduta su di loro, hanno cambiato atteggiamento ed hanno cominciato a fare pressione sulla direzione per realizzare investimenti e per conseguire la certificazione.

La situazione è comunque variegata: c'è chi persegue il minimo sindacale per poter comunque essere coperto, e chi invece, particolarmente sensibile su queste tematiche, implementa sistemi di gestione, infrastrutture ben gestite, usa servizi SOC e SIEM. In questi casi l'azienda capisce che gli oneri per la cybersecurity non sono costi, ma sono investimenti.

L'autorefenzialità non basta

A livello statistico le software house sono le meno certificate 27001, ha specificato Genna. Quelli che hanno approcciato la 27001 e si sono certificati hanno naturalmente dovuto affrontare due aspetti: la parte di *vulnerability assessment* sui sistemi; la parte di *vulnerability assessment* sulla dimensione applicativa. Però permane ancora un alto numero di aziende che continua a lavorare sull'autoreferenzialità. Ma il mercato sta cambiando, ha aggiunto. Adesso, infatti, i grandi clienti di questa autoreferenzialità se ne fanno poca cosa e chiedono o la certificazione - in questo caso una 27001 - oppure le validazioni del software secondo delle linee guida. Inoltre, i grandi operatori negli anni hanno pensato di fare contratti stringenti, con tutta una serie di garanzie per ribaltare sul fornitore eventuali responsabilità. Si è innescato un circolo che probabilmente con la NIS II verrà rivisto ed il mercato prossimamente potrebbe avere un'evoluzione positiva.

Intelligenza artificiale e norme tecniche

In merito alla norme tecniche sull'AI, Genna ha spiegato che la ISO ha pubblicato la 42001/2023 sulla gestione dell'intelligenza artificiale da parte delle organizzazioni ed ha individuato tre soggetti: gli sviluppatori, quindi chi crea applicativi da rivendere sul mercato; i fruitori, le aziende che acquistano l'intelligenza artificiale e la applicano al proprio processo produttivo; e poi gli sviluppatori fruitori, generalmente grandi aziende con divisioni al proprio interno che sviluppano l'intelligenza artificiale che poi applicano all'interno dei propri processi.

Mario Finetti

La difficoltà di scegliere le priorità per difendersi

Mario Finetti ha riferito della sua esperienza ventennale nel gruppo Eni, dove ha lavorato principalmente all'estero: tre anni e mezzo in Kazakistan, sei anni in Nigeria, un anno in Ghana e tre anni e mezzo in Egitto. Ha aggiunto di essere rientrato in Italia l'anno scorso per far parte di

Colacem, del gruppo Financo. Ha detto di ritenere che la consapevolezza delle aziende riguardo alla Cyber, con tutti gli attacchi che si sono visti, sia abbastanza alta nelle aziende industriali.

È facile sbagliare però – ha aggiunto - quando si tratta di scegliere la priorità degli interventi. Spesso si investono tantissime risorse in una direzione per correggere un determinato problema che effettivamente esiste, ma si sottovaluta un'altra cosa che richiede attenzione.

Nel mondo Cyber, ha sottolineato, è difficile distribuire le risorse. Prioritarizzare gli interventi non è banale, è un esercizio che richiede una certa consapevolezza e anche un po' di fortuna. Si può fare un lavoro bellissimo al 99% della superficie aziendale, ed essere poi attaccati sull'1% che è stato un po' trascurato.

Poi c'è il tema assolutamente importante – ha proseguito Finetti - della catena dei fornitori, esasperato dal cloud, perché è evidente che i fornitori di servizi applicativi in modalità cloud sono da tenere particolarmente sotto la lente di ingrandimento.

Il fatto di interagire via internet con le società e con i service provider merita una particolare attenzione. Non si può pensare di trasferire quello che prima funzionava all'interno della propria rete in un servizio internet, con le stesse modalità e con lo stesso livello di protezione che aveva quando era protetto dal perimetro aziendale, perché pubblicare una cosa su internet richiede un livello di protezione e di consapevolezza molte volte più alto rispetto a far funzionare un servizio on premise.

Il passaggio dall'offerta del software in modalità licenza alla modalità cloud, seppur più redditizio per le imprese fornitrici, apre infatti molti problemi legati alla sicurezza, perché le software house spesso non hanno le competenze tecnologiche necessarie per garantirla.

Finetti ha infatti menzionato che sta rifiutando molte offerte di migrazione al cloud perché proposte da aziende che non offrono adeguate garanzie di gestione degli aspetti di cybersecurity.

Le aziende nate con un certo tipo di mestiere non possono riconvertirsi in cloud company in un anno. Rischiano di essere purtroppo oggettivamente un po' indietro e dovrebbero valutare con molta attenzione la situazione prima di offrire i propri servizi in modalità cloud.

Un altro tema importante che riguarda soprattutto le aziende industriali, ha sottolineato, è imparare a vedere il contributo degli auditor, di chi fa consulenza in ambito cybersecurity, come un contributo positivo. La resistenza al cambiamento è infatti un tema importante anche nella cybersecurity. Accettare un consiglio da un esterno è molto importante e può far crescere e migliorare molto l'organizzazione; mentre, viceversa, resistere ai consigli, insistere sul fatto che si è nel migliore dei mondi possibili, è un atteggiamento rischioso, un atteggiamento che fa perdere tempo e che fa perdere opportunità di crescita.

Finetti ha parlato dell'importanza di definire un *threat model* per capire da che cosa ci si vuole proteggere; fare una *business impact analysis* per capire cosa le unità di business possono fare e cosa non possono fare in assenza dei sistemi informativi, ed, infine, arrivare a definire un *return point objective* per comprendere se va bene fare un backup una volta al giorno o è necessario avere una *continuous data protection,* perché in caso di problemi bisogna essere in grado di ritornare all'ultima transazione di 10 minuti prima dell'incidente. Queste cose possono essere valutate solo facendo un percorso abbastanza articolato e complesso con tutte le unità di business

impattate e poi, ovviamente, i piani di *disaster recovery* devono essere testati almeno una volta all'anno.

In merito all'intelligenza artificiale applicata alla Cyber, Finetti ha sottolineato come in taluni casi il contributo umano delle risorse aziendali non possa essere sostituito non solo dalla tecnologia, ma neanche esternalizzato.

Alessandro Calabrese

Competenze di cybersecurity nelle PMI

Alessandro Calabrese ha spostato l'attenzione sulle competenze in materia di cybersecurity, evidenziandone la mancanza, a livello mondiale. Secondo una recente indagine, l'80% degli incidenti di cyber deriva da una carenza di competenze.

Soprattutto all'interno delle piccole e medie imprese si rileva questa lacuna. Il centro di competenza Cyber 4.0 – ha aggiunto - sta lavorando per colmare questo divario. La formazione rappresenta infatti circa il 37% dei servizi offerti.

Tra i servizi finanziati dal PNRR vi è una richiesta altissima di formazione da parte dell'alta direzione, che poi dovrebbe dare luogo ad un trasferimento di conoscenze per formare e rendere consapevole anche il resto della popolazione aziendale.

Grazie ai fondi Next Genenation EU, Cyber 4.0 può erogare servizi in materia di Cybersecurity – con la cosiddetta linea B2 - con intensità di aiuto pubblico per le PMI che può arrivare fino al 100%. Tra l'altro, le piccole e medie imprese saranno direttamente coinvolte nella NIS II come fornitori di infrastrutture critiche nazionali, ed anche come produttrici o fornitrici di servizi essenziali.

Il Cyber Resilience Act

Le piccole e medie imprese, ha proseguito Calabrese, saranno interessate da altre normative, quali, per esempio, il Cyber Resilience Act. I produttori di beni con elementi digitali al proprio interno saranno chiamati a rispondere a un determinato schema certificativo per poter immettere i loro prodotti sul mercato. Quindi è molto importante capire che anche la piccola e media impresa dovrà necessariamente mettersi nell'ottica di creare dei processi di governance in grado di poter rispondere a queste esigenze normative che rispondono a dei rischi reali.

Per affrontare un problema di elevata complessità come la gestione della sicurezza delle informazioni bisogna partire dalle basi: capire quali sono gli asset che vanno protetti; cosa c'è in casa; poi, dopo, andare ad acquistare la tecnologia di protezione, ha concluso Calabrese.

Conclusioni

L'incontro ha evidenziato l'importanza cruciale della cybersecurity e della gestione delle vulnerabilità all'interno delle aziende. Gli interventi dei relatori hanno sottolineato come la consapevolezza e la preparazione siano fondamentali per affrontare gli incidenti e minimizzare i rischi. È emerso che molte aziende ancora non comprendono pienamente l'importanza di avere un *incident response plan* e di fare simulazioni di attacchi *ransomware*. Inoltre, è stato discusso il ruolo delle direttive, quali la NIS II, e delle certificazioni, come la ISO 27001, per garantire la

sicurezza delle informazioni, ed è stata sottolineata la necessità di vedere gli investimenti in sicurezza come investimenti e non come costi.

L'intelligenza artificiale è stata riconosciuta come uno strumento potente per la cybersecurity, ma è stato anche sottolineato che deve essere utilizzata con intelligenza umana e che può rappresentare un rischio se utilizzata dagli attaccanti. È stato evidenziato che l'intelligenza artificiale può aiutare nella rilevazione e gestione degli eventi di cybersecurity, ma che è necessario monitorarla costantemente per evitare vulnerabilità.

Infine, è stato discusso il problema della mancanza di competenze di cybersecurity all'interno delle aziende, soprattutto nelle piccole e medie imprese, e l'importanza della formazione per colmare questo divario. È stato sottolineato che la gestione della sicurezza richiede un approccio sistemico che coinvolga tutte le unità aziendali e che la consapevolezza e la preparazione sono fondamentali per affrontare i rischi di cybersecurity.

Glossario per inglesismi

Accountability: Responsabilità
Adaptability: Adattabilità
AI: Intelligenza Artificiale
Analysis Of The Evolution Of The Specifications: Analisi dell'evoluzione delle Specifiche
Backup: Copia di Sicurezza
Business Continuity: Continuità Operativa
Business Impact Analysis: Analisi dell'impatto Aziendale
Classification: Classificazione
Cloud: Nuvola Informatica
Compliance: Conformità
Continuous Data Protection: Protezione Continua Dei Dati
Cybersecurity: Sicurezza Informatica
Data Processing: Elaborazione dei Dati
Digital Maturity: Maturità Digitale
Digital Transformation: Trasformazione Digitale
Disaster Recovery: Recupero da Disastro
EDR: Rilevamento d Risposta degli Endpoint
Ethics: Etica
Governance: Gestione
HR: Risorse Umane
Human Centric: Centrato sull'uomo
Industry 4.0: Industria 4.0
Matchmaking: Abbinamento
NIS II: Direttiva NIS II
On Premise: In sede
Predictive Capability: Capacità Predittiva
Privacy: Riservatezza
Quick Win: Vittoria Rapida
Quotes: Preventivi
Ransomware: Software Malevolo
Return Point Objective: Obiettivo di Punto di Ritorno
Roadmap: Piano d'azione
Scalability: Scalabilità
Security Operation Center: Centro Operativo di Sicurezza
Supply Chain: Catena di Fornitura
Tagging: Etichettatura
Technical And Commercial Proposal Processing Times Reduction: Riduzione dei Tempi di Elaborazione Delle Proposte Tecniche e Commerciali
Technical Documentation: Documentazione Tecnica
Threat Model: Modello di Minaccia
Time Reduction In Preparation And Revision For Technical Documentation: Riduzione dei Tempi di Preparazione e Revisione della Documentazione Tecnica
Transparency: Trasparenza
User Manuals: Manuali Utente
Utility: Servizi Pubblici
Value Chain: Catena Del Valore

Value Sensitive Design: Progettazione Sensibile ai Valori
Visibility: Visibilità
XDR: Rilevamento e Risposta Estesa