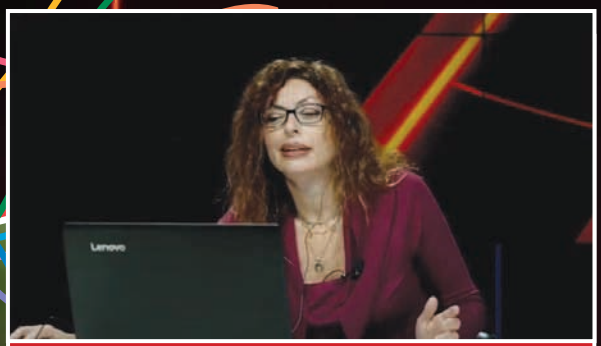
secsolutionforum
The digital event for the security industry

Ilaria Garaffoni

Sicurezza fisica: dal Covid al green passando per l'IT e il GDPR

"*Sicurezza fisica, sicurezza logica e privacy: si riparte dal Covid?*" - questo il titolo della tavola rotonda d'apertura di *secsolutionforum 2021*, che ha visto schierati alcuni rappresentanti del mondo della sicurezza fisica (**Giulio Iucci,** Presidente di ANIE Sicurezza), della sicurezza logica (**Alvise Biffi,** Coordinatore Steering Commettee Cyber Security di Assolombarda), della sicurezza dei dati (**Luciano Corino,** Membro del Consiglio Direttivo di Federprivacy) e della grande utenza (**Alessandro Manfredini,** Vice Presidente AIPSA - Associazione Italiana Professionisti della Security Aziendale). Un parterre d'eccezione che coagulava le quattro "gambe" di un settore che si intreccia con mondi tangenziali (cyber, dati, sicurezza logica) in modo sempre più pervasivo e, soprattutto dopo una pandemia che ha posto la digitalizzazione al centro dei processi, non può più permettersi di pensare in modo autoreferenziale.



ILARIA GARAFFONI – Responsabile di redazione di Secsolution Magazine

ALVISE BIFFI – Coordinatore Steering Commettee Cyber Security di Assolombarda

Una tavola rotonda di confronto e contaminazione per generare idee nuove

LUCIANO CORINO – Membro del Consiglio Direttivo di Federprivacy

GIULIO IUCCI – Presidente ANIE Sicurezza

ALESSANDRO MANFREDINI – Vice Presidente AIPSA

Covid: lesson learned?

Si è partiti dal grande convitato di pietra: il Covid. Quale lezione ci ha insegnato? Una volta cessata l'emergenza, cosa resterà delle tecnologie di sicurezza messe in campo per combattere la pandemia? La massificazione (intesa come esposizione mediatica e applicativa nel settore consumer) acquisita dalle tecnologie di sicurezza fisica ha posto il settore al centro della scena: saremo capaci di capitalizzare questa centralità ad emergenza cessata? E sapremo gestire le debolezze poste da un'integrazione sempre più spinta con il mondo IT e i rischi cyber?

Il Covid ha mostrato a tutti, con brutalità, quanto costa la non sicurezza – ha detto Iucci. Le tecnologie di sicurezza fisica sono state abilitanti e la pandemia le ha rese di linguaggio comune, sdoganando e portando nel quotidiano prodotti, ma anche logiche e concetti estranei al grande pubblico (rischio, crisi, procedure, emergenza, prevenzione). Aziende e professionisti che si sono sempre occupati di resilienza e contenimento della crisi sono diventati interlocutori di riferimento: il punto nodale oggi è dunque la professionalità, essenziale per veicolare questo modello su altre tecnologie ed applicazioni.

Cyber security by design e privacy by design come nuovi elementi premiali di competitività

Al settore informatico il Covid ha insegnato che la resilienza è senza dubbio utile, ma che la programmazione è decisamente meglio – ha chiosato Biffi. Chi era già preparato al remote working ed alla gestione allargata della sicurezza fisica e logica ha gestito meglio una digitalizzazione spinta o accelerata dal Covid. *Non si inventano i processi da un giorno all'altro,* ha proseguito Biffi: alla base della tecnologia deve esserci un processo organizzativo logico cui asservire la tecnologia, tale per cui la cyber security possa diventare un elemento competitivo e non l'ennesimo balzello. Se al cliente arriva il messaggio che il dato è sicuro, la cyber diventa competitiva.

Per i security manager il Covid è stato una grande opportunità, ha dichiarato Manfredini: le aziende si sono affidate alla funzione di security e il manager è stato riconosciuto come un *regista* capace di lavorare in ambienti ad alto tasso di stress per garantire la sicurezza della forza lavoro e la continuità dell'erogazione dei servizi. "Abbiamo coordinato team molto verticali, con il coinvolgimento del medico competente e dello staff HSE, combinando esigenze di safety con security e compliance, tra l'altro con una normativa che cambiava giorno dopo giorno. Sono prevalsi i soft skill, le capacità manageriali e il saper pensare in modo olistico".

Opportunità dunque, ma anche un banco di prova non sempre positivo per la sicurezza fisica, quanto meno sotto il profilo della compliance. "Il Covid ha portato in luce anche gli errori più marchiani di progettazione e costruzione dei dispositivi in termini di privacy by design – ha avvertito Corino. La protezione dei dati è un diritto di libertà: alcuni sistemi di riconoscimento facciale negano l'accesso a soggetti con alcune caratteristiche somatiche, aprendo la porta a discriminazioni ideologiche inaccettabili. La privacy by design è dunque anche un tema di democrazia. Come lo è, a ben vedere, quello della sicurezza logica – tema che ha spalancato le porte ad una nuova domanda.

Violazioni cyber di sistemi di sicurezza fisica: chi paga?

Dall'inizio della pandemia sono aumentati i problemi di sicurezza cyber rilevati all'interno dei sistemi di sicurezza fisica. Ma chi risponde per le violazioni cyber dei sistemi di sicurezza fisica? Al di là della norma, quali e quante teste possono rotolare in un mondo sempre più interconnesso, dove la catena delle responsabilità (immaginiamo un organismo ipercomplesso come la smart city) si fa sempre più sfumata?

"Sono in tanti a dover pagare – risponde Iucci: il security manager, il responsabile della sicurezza logica, il responsabile dei sistemi informativi, il data protection officer, l'amministratore di sistema, fino all'amministratore delegato. Credo che, per non far rotolare teste, bisognerebbe non solo stabilire le procedure, ma ragionare in termini di convergenza tra sicurezza fisica e logica con architetture e best practise ad hoc".

Buon senso by design per un trust di filiera allargata (cit. Manfredini)

"Tutti responsabili, conferma Biffi, *ma bisogna identificare l'ambito"*. Se consideriamo non un'azienda ma una smart city ci troveremo ad analizzare un ecosistema interconnesso dove le figure sono potenzialmente infinite: dal produttore di TVCC al gestore del servizio, dall'infrastruttura cloud al protocollo di comunicazione, e tanto altro ancora. Come capire quindi chi è responsabile? "Bisogna analizzare da dove origina il problema - che spesso deriva da concause - e da lì partire con la catena di responsabilità". E bisogna pensare ad una cyber security by default, che inserisca la sicurezza logica già in fase di progettazione perché gestire una violazione a posteriori è complesso, dispersivo e talvolta controproducente.

Secondo gli esperti di GDPR e privacy, le responsabilità si allocano in tutti coloro che hanno contribuito a generare (o non hanno contribuito a limitare) una data leak/breach. Quindi, risponde senza dubbi Corino, dove c'è fuga/accesso non autorizzato di dati, personali o meno, c'è una responsabilità condivisa tra più figure. Escludendo il DPO perché si tratta di un'autorità di controllo, sono inclusi tutti gli attuatori dei processi di trattamento dei dati personali, soprattutto se a monte ci sono errori marchiani di progettazione/costruzione degli strumenti in termini di privacy by design.

Netto Manfredini: la responsabilità è del legale rappresentante dell'azienda. Ma se anziché fare una caccia alle streghe si rafforzasse un trust tra le parti tale da distribuire su tutti i manager il principio dell'accountability, anche al netto del dettato della norma? Una sorta di "buon senso by design"?

Un manifesto della sicurezza

La provocazione di Manfredini ha portato dritti ad un altro tema: quello del trust, del buon senso by design appunto, dell'elaborazione di un documento programmatico, di un 'manifesto' che coinvolga le varie figure chiave al fine di concertare delle best practise in materia di sicurezza logica dei sistemi di sicurezza fisica, con uno sguardo attento al GDPR e alla privacy.

Tutti d'accordo su questo punto: in ANIE si sta già ragionando ad un tavolo permanente di filiera e il Presidente si è detto pronto ad allargarlo ad altre figure chiave e ad altri temi chiave, come il green e la transizione ecologica – vera bandiera ideologica del Recovery Fund, curiosamente depositato dal Governo Draghi proprio nelle giornate del forum. La domanda successiva era quindi d'obbligo.

Security goes green?

Nelle condizionalità all'impiego del Recovery Fund, la Commissione Europea ha posto l'accento sull'impatto ambientale. Un tema che non lascia esente il comparto IT: il tema del green computing, o informatica ecologicamente sostenibile, è da tempo al centro del dibattito. Ma è un tema che coinvolge da vicino anche il comparto sicurezza: in che modo il nostro settore può dare un contributo al green value e alla protezione ambientale? Il green si può considerare un driver di sviluppo (anche in termini di argomentazione di marketing) per la sicurezza fisica?

"Il settore sicurezza sta sviluppando da tempo i prodotti in materiali più ecosostenibili, la raccolta RAEE è rispettata e le stesse tecnologie di videosorveglianza permettono di vigilare sul rispetto dell'ambiente con sistemi di monitoraggio continuo" - risponde Iucci. Altro tema green sono le microtecnologie (la miniaturizzazione degli apparati riduce l'impatto ambientale) e la scelta di ridurre l'hardware di campo, di aumentare la remotizzazione e l'incorporazione di tecnologia a bordo. "Cloud e 5G ci aiuteranno a ridurre gli apparati a campo per concentrarli nello storage, nell'analisi on board. La stessa intelligenza artificiale permette di accentrare sulla macchina moltissime funzioni, riducendo l'impatto ambientale- conclude Iucci.

Security goes green: meno hardware, più microtecnologie, centralizzazione, cloud e focus sui consumi

Biffi si spinge oltre: "la base della sostenibilità, o economia circolare, è immaginare il fine vita di un prodotto già nel momento in cui lo si sta progettando. Semaforo verde quindi a materiali green, efficienza di progettazione ed efficientamento di servizio e di energia (smart metering, smart greed)". L'aspetto normativo è però problematico, visto che ogni paese segue logiche diverse, avverte Biffi. La vera sfida è quindi che il cliente percepisca la sfida della sostenibilità come valore di sviluppo commerciale, come elemento di competitività, magari ipotizzando dei premium price.

La stessa privacy potrebbe e dovrebbe diventare un elemento competitivo. In una logica green, Corino rileva che anche gestire e trasmettere dei dati presenta un conto ambientale. La privacy by design può dunque dare un piccolo contributo non limitando la circolazione dei dati, ma limitando la quantità di dati che inutilmente - o peggio illecitamente - vengono trasmessi.

La conclusione è toccata a Manfredini: "la transizione ecologica è il tema del presente se vogliamo avere un futuro, quindi digitalizzazione e fine vita dei prodotti in una logica no waste sono essenziali, ma attenzione ai consumi di grandi data center e cloud. Il focus deve quindi essere puntato sulle fonti energetiche rinnovabili".

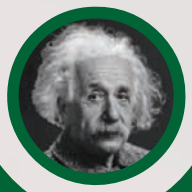
Rapporto uomo - macchina
Commento dei relatori a frasi celebri

"La sicurezza dipende non tanto da quanto hai, ma da quanto puoi fare senza."
Joseph Wood Krutch

"Cosa sono disposto a perdere? Quanto costa la non sicurezza? Il Covid ce l'ha insegnato" Giulio Iucci

"Un giorno le macchine riusciranno a risolvere tutti i problemi, ma mai nessuna potrà porne uno."
Albert Einstein

"Ben venga l'uomo con i suoi dubbi eterni", commenta Luciano Corino. *"E attenzione, parlando di intelligenza artificiale, alla stupidità artificiale"*, chiosa Alvise Biffi.



"Le macchine mi colgono di sorpresa con grande frequenza."
Alan Turing

"...soprattutto quando attraverso sulle strisce pedonali con il semaforo rosso! - commenta Alessandro Manfredini: *occorre sempre governare le macchine, porle al nostro servizio e non farci cogliere di sorpresa dalla tecnologia commettendo errori marchiani.*