Paolo Dal Cin (Accenture): ‘La cybersecurity non un costo, ma opportunità di business per le aziende’

“Siamo in uno scenario di cyberspace sempre più complicato con nuove minacce e con un cybercrime più aggressivo e attacchi a livello governativo che colpiscono infrastrutture critiche supply chain e terze parti”, descrive così il momento storico, nella videointervista condotta da **Eliana D’Aquanno**, **Paolo Dal Cin**, attuale Managing Director di **Accenture Security** con responsabilità per l’Italia, Europa Centrale e Grecia (ICEG), e di recente nominato Security Lead per l’Europa e l’America Latina.

Quale uno dei migliori strumenti di cybersecurity per proteggere le infrastrutture critiche nazionali? *“La direttiva Nis”*, ha aggiunto Dal Cin.
La Direttiva europea nota come “**Nis**”, Network and Information Security, per la prima volta a livello europeo affronta in modo organico e trasversale il tema della cybersecurity, contribuendo ad incrementare il livello comune di sicurezza nei 28 Paesi membri.

“La direttiva Nis è un faro” ha spiegato Dal Cin, *“ma il livello di applicazione della normativa è fortemente limitata per la scarsa attenzione dedicata al tema e invece più concentrata al Regolamento Ue per la protezione dei dati”.*

“L’Italia ha la necessità di proteggere le infrastrutture critiche nazionali, energetiche, Tlc e sistemi interbancari” ha detto il manager di Accenture, sottolineando che “*la cybersecurity non è un costo, ma opportunità di business per le aziende per abilitare nuove opportunità legate*

all'Innovazione'.

https://www.key4biz.it/paolo-dal-cin-accenture-la-cybersecurity-non-un-costo-ma-opportunita-di-business-per-le-aziende/251660/

Virus Melissa: 20 anni dopo cosa abbiamo imparato?

*La rubrica **AssetProtection**, ovvero Riflessioni su sicurezza e terrorismo, a cura di Anthony **Cecil Wright**, presidente Anssaif (Associazione Nazionale Specialisti Sicurezza in Aziende di Intermediazione Finanziaria). Per consultare gli articoli precedenti **clicca qui**.*

Il 26 marzo del 1999 iniziò a diffondersi un virus, creato da un tale **David Lee Smith**, che infettò oltre 1 milione di sistemi; provocò danni diretti stimati in oltre 80 milioni di dollari e bloccò, anche per diversi giorni, l'operatività dei server mail di oltre 300 grandi aziende ed enti governativi.

Il programmatore Smith, ammiratore della bella striptease Melissa, prese possesso di un *account* di AOL e lo utilizzò per pubblicare un file in un gruppo Internet chiamato "alt.sex", promettendo decine di password per accessi gratuiti a siti che forniscono materiale non idoneo per i minori. Una volta aperto il documento Word, il virus si diffondeva nel computer e quindi, utilizzando Outlook, si spediva agli indirizzi email trovati. La email spedita suggeriva al destinatario di aprire il documento allegato che aveva un nome del tipo "sexxxy.jpg" oppure "naked wife".

Già 20 anni fa il phishing sfruttava anche email inviate da persone conosciute!

La velocità di propagazione e i problemi creati misero in allarme l'FBI che sollecitò tutti a porre attenzione alle email ed ai relativi allegati.

Fu questo il primo episodio di una certa gravità? No.

Un grave episodio era già avvenuto 11 anni prima! Infatti, il 2 novembre del 1988 un worm (conosciuto come **Morris worm**) si diffuse su Internet: nelle prime 24 ore aveva già bloccato circa il 10% dei computer connessi in rete. Colpiti furono i sistemi UNIX del Massachusetts Institute of Technology (MIT), e di Harvard, Princeton, Stanford, Johns Hopkins, NASA, ed il Lawrence Livermore National Laboratory.

Oltre a sfruttare una porta ed un problema nel software di identificazione degli utenti in rete, era progettato anche per stare nascosto.

Domanda: gli utilizzatori hanno finalmente compreso la lezione?

Scrive il CLUSIT:«*Tutti gli analisti ed esperti di sicurezza concordano* ***che la maggior parte degli incidenti di sicurezza è legata ad errori umani*** *(si stima che siano circa l'80%-90% degli incidenti) confermando come il fattore umano sia, anche per la sicurezza informatica, l'anello debole del sistema. Solo in Italia si è stimato che circa il 53% degli attacchi sono dovuti a cause endogene (****utilizzo di password deboli e non alfanumeriche, accesso di device aziendali a connessioni pubbliche, navigazione in siti non sicuri e il trasporto di dati sensibili con chiavi USB non cifrate****,…) e a queste si sommano gli attacchi di phishing e spear phishing che provocano impatti significativi sull'azienda sia in termini di*

frodi e dati rubati che come incremento dei costi operativi per il ripristino dagli incidenti occorsi.».

Conclusione: 1988, 1999, 2019: nulla è cambiato nell'atteggiamento del cittadino?

Vi è però, a mio parere, una eccezione che fa piacere. Nell'ambito della mia attività presso l'AGID mi è capitato di leggere la esigenza, manifestata dal management di diversi Enti della Pubblica Amministrazione, di far frequentare corsi di sensibilizzazione ad attacchi di Social Engineering a tutto il personale, IT incluso. Ottimo!

Ma ciò a mio parere non basta, in quanto bisogna far sì che l'attenzione alle minacce entri nel DNA delle persone.

Che fare quindi?

La soluzione a mio parere è di iniziare a **diffondere la cultura dell'attenzione ai rischi iniziando dai ragazzi, se non addirittura dai più piccoli.**

Nel prossimo articolo racconterò della mia esperienza con decine di classi medie inferiori in due regioni italiane.

Anthony Cecil Wright

https://www.key4biz.it/virus-melissa-20-anni-dopo-cosa-abbiamo-imparato/251563/

Cybercrime, Confindustria avverte: 'Italia vulnerabile

per il basso livello di e-skill’

Non solo Pil azzerato e recessione economica che fotografa una “Italia ferma”, il Centro Studi Di Confindustria lancia anche l’allarme sulla sicurezza informatica del nostro Paese.

Secondo quanto afferma il **Centro Studi di Confindustria** nel suo rapporto di primavera presentato questa mattina “*la minaccia cibernetica a livello globale è destinata a crescere, di pari passo con la progressiva digitalizzazione della società e l’evoluzione degli strumenti di attacco. E l’Italia è “particolarmente vulnerabil*e”.

Lo studio ha quantificato che il costo degli attacchi cibernetici potrebbero mettere a rischio inoltre i benefici economici della digitalizzazione: nel 2030 potrebbero infatti arrivare a pesare per l’1,2% del Pil mondiale.

Secondo quanto afferma il Centro Studi di Confindustria,” *l’Italia, dato che si trova al 25/o posto su 28 in Europa per livello di competenze digitali, è per questo “particolarmente vulnerabile agli attacchi”*.

Nel corso del 2018 gli attacchi cibernetici si sono quintuplicati, colpendo a largo spettri diversi settori economici, con in testa quello dall’energia (11% del totale), seguito dai trasporti e da telecomunicazioni e finanza.

Inoltre secondo i recenti sondaggi il 39% degli italiani ha subito un reato o conosciuto una vittima del cybercrime (in linea con la media globale).

Le preoccupazioni maggiori che provengono dai cittadini sono il furto d’identità (81%) e dall’hacking dei social media

(80%).

Tra i crimini più temuti seguono poi le transazioni fraudolente bancarie o su carta di credito (71%), false chiamate, mail e sms (70%), il furto dell'account e gli acquisti online fraudolenti (68%).

https://www.key4biz.it/cybercrime-csc-avverte-italia-vulnerabile-a-causa-del-livello-basso-di-competenze-digitali/251472/

Cyber attacchi potrebbero costare al Regno Unito più di un miliardo di sterline l'anno

In media, ogni singolo attacco informatico subito dalle imprese britanniche durante il 2018 è durato 67 minuti, per un costo complessivo di circa 140 mila sterline. È quanto riportato nella quattordicesima edizione del "***Worldwide Infrastructure Security Report (WISR)***" Netscout, secondo cui **il Regno Unito, da qui in poi, potrebbe dover sostenere più di un miliardo di sterline l'anno di costi per cyber attacchi**.

Sette i Paesi presi in esame dai ricercatori, per tipologia di attacchi, target, tecniche, danni e costi: Stati Uniti, Francia, Canada, Brasile, Regno Unito, Germania e Giappone.

"*Ogni azienda britannica è dotata di decine di strumenti per la cybersicurezza e gli investimenti in nuove tecnologie e soluzioni stanno aumento rapidamente, senza però risolvere davvero il problema*", ha spiegato **Darren Anstee**, CTO Security

di Netscout.

“*Le organizzazioni, infatti, hanno la necessità di sviluppare una visione d’insieme delle loro risorse più integrata, con una logica di armonizzazione tra risorse virtuale, fisiche e cloud. Fondamentale in questo frangente storico è rivolgersi a consulenti esterni, che possono fornire anche un aiuto per organizzare e formare le risorse interne*”.

I servizi aziendali *cloud-based* hanno visto passare gli attacchi **DDoS**, acronimo *di Distributed Denial of Service* (interruzione distribuita del servizio) dal 25% nel 2017 **al 47% nel 2018**.

Non è tanto il numero in generale di attacchi DDoS a colpire i ricercatori (anzi, in calo del 4% su base annua a 6,13 milioni), quando le dimensioni e la complessità di ognuno di essi, aumentate del 273%.

I service provider hanno visto passare gli attacchi alle piattaforme governative dal 37 al 60%.

Il costo medio di un’ora di interruzione di servizio ha raggiunto quasi i 222 mila dollari per azienda a livello mondiale: il record è stato registrato in Germania, con quasi 352 mila dollari l’ora, mentre il costo più basso in Giappone, poco più di 123 mila dollari.

> *Cyber attacchi potrebbero costare al Regno Unito più di un miliardo di sterline l’anno*

La diffusione della cultura del rischio, come si comportano le imprese?

*La rubrica **AssetProtection**, ovvero Riflessioni su sicurezza e terrorismo, a cura di Anthony **Cecil Wright**, presidente Anssaif (Associazione Nazionale Specialisti Sicurezza in Aziende di Intermediazione Finanziaria). Per consultare gli articoli precedenti **clicca qui**.*
Cattivi esempi.

Un professionista si chiedeva su un social, pochi giorni fa, come mai i servizi di una grande banca possano essere stati fermi per quasi 36 ore, per quale causa ed oltretutto perché non abbia fornito una comunicazione ai clienti.

Nessuno ha potuto operare né con lo smartphone, né con il PC su Internet, né andando in agenzia: anche i dipendenti non potevano operare sui conti.

Nessuna comunicazione ufficiale, tranne – dopo una decina di ore di blackout – un "cartello", a livello online e mobile, che avvisava che a breve (24 ore dopo!) il servizio sarebbe ripreso.

Sembra che ciò sia stato dovuto ad un problema causato da una società di sviluppo software che aveva in corso i test di una nuova procedura. La stessa fonte ha affermato che degli hacker abbiano trovato modo di entrare nei sistemi e fare dei non meglio precisati danni (copiati i dati?). Un'altra fonte interna ha accennato invece ad un serio problema di trasmissione dati (blackout di 36 ore? Possibile?). Quindi, in conclusione, non sappiamo quale sia stata la reale causa.

Perché ho citato questo episodio? Per cogliere l'opportunità di scambiare alcune considerazioni con i lettori, proponendo i seguenti interrogativi:

1. L'assenza di comunicazione ai clienti e stakeholders e i lunghi tempi per il ripristino di almeno alcuni servizi essenziali, non sta ad indicare che i piani di *business continuity e crisi management* non hanno funzionato o sono oramai un ricordo dei bei tempi passati?
2. Quante aziende sono nelle stesse condizioni?
3. Qualora un malware o degli hacker avessero effettivamente approfittato di qualche "porta" aperta su un server, a causa della concentrazione del personale sui test della nuova applicazione trascurando la sicurezza, non vorrebbe dire che l'esperienza recente (un noto ospedale romano) e quella passata (anni fa nella stessa azienda), non insegnano nulla?
4. Si parla, giustamente, di diffondere una adeguata cultura dei rischi informatici, ma è possibile che vi siano delle grandi aziende che non rispettano le norme più elementari?
5. L'esperienza insegna che la fretta di mettere in produzione una applicazione (pur giustificata dalla guerra alla concorrenza), non accompagnata da adeguate misure preventive e di *contingency*, continua a mettere a rischio la sicurezza dei cittadini. Non solo in banca. Il caso recente della Boeing non è drammaticamente eclatante?
6. Altresì grave è che l'esperienza passata non abbia alcun valore. Perché il personale con molta esperienza non viene incentivato a trasferire le sue esperienze ai più giovani? Perché non si fa tesoro dell'esperienza?

Credo che sia necessario un momento di riflessione.

Mi farebbe piacere ricevere un vostro parere.

Anthony.wright@anssaif.it

https://www.key4biz.it/la-diffusione-della-cultura-del-rischio-come-si-comportano-le-imprese/250873/

Facebook, nuova falla di sicurezza per gli utenti. 600mila password alla mercé dei dipendenti di Menlo Park

I problemi per **Facebook** non finiscono più: un nuovo scandalo relativo alla sicurezza e alla privacy sta colpendo il social network più famoso al mondo.

Quasi 600 milioni di account sono a rischio a causa di una falla di sistema: tantissime password sono state salvate in un normale documento di testo privo di alcuna forma di sicurezza o criptografia, completamente accessibile a tutti i dipendenti della società di **Mark Zuckerberg.**

L'errore è stato ammesso e rivelato sul blog ufficiale di Facebook da **Pedro Canahuati**, VP Engineering, Security and Privacy del social network.

La falla di sicurezza

Tutto è partito da una denuncia firmata dai ricercatori di **KrebsOnSecurity,** secondo i quali le password di milioni di utenti di Facebook sarebbero state archiviate in testo normale e finite alla mercé dei circa 20mila dipendenti dell'azienda nel cloud aziendale.

Semplici file a portata di click, senza alcuna protezione con le probabilità che le password utilizzate per accedere a Facebook siano uguali a quelle utilizzate per gli altri servizi.

Secondo Facebook, non ci sono prove che le password in chiaro siano state esposte al di fuori della società, o che siano state utilizzate dai dipendenti per accedere agli account.

Perciò agli utenti non sarà richiesto di reimpostare le proprie password. Da Menlo Park fanno sapere, inoltre, "*che il problema ha colpito centinaia di milioni di utenti di Facebook Lite, decine di milioni di altri utenti di Facebook, e decine di migliaia di utenti di Instagram*".

Per la vostra sicurezza cambiate password

Se usate Facebook, il consiglio è non solo di cambiare password ma farlo anche per gli account di altri servizi, soprattutto se avete il vizio di usare le stesse password per più servizi. L'ideale sarebbe usare password esclusive per gli account più importanti, soprattutto per la posta elettronica, i conti online e i social network e quando è possibile, attivate sempre la verifica a due fattori.

L'ennesimo scivolone

Oramai gli scandali sulla privacy di Facebook non fanno più nessun rumore.

Non è bastato Cambridge Analityca, l'attacco hacker di ottobre 2018 che ha visto coinvolti 90 milioni di utenti, o la cessione dei dati a terze parti che vede Facebook indagato

dalla Corte Federale di New York (l'ultima in ordine di arrivo)

Proprio adesso che Mark Zuckerberg è diventato il paladino della privacy con il suo nuovo progetto di fondere Facebook, Instagram e WhatsApp (alla faccia della privacy) il CEO prende un altro scivolone, l'ennesimo.

Non riusciamo a capire perché un'azienda che ha 2 miliardi di utenti registrati e con un fatturato di 41 miliardi di dollari (dati 2017) non riesca a proteggere minimamente i propri utenti.

Incompetenza forse? O consapevolezza del valore immenso che hanno i dati degli utenti per poter aumentare il fatturato?

https://www.key4biz.it/facebook-nuova-falla-di-sicurezza-per-gli-utenti-600mila-password-alla-merce-dei-dipendenti-di-menlo-park/250841/

Privacy. Snowden: 'La crittografia end-to-end non basta, Apple&Co. hanno ancora gravi vulnerabilità'

"*Il mio lavoro oggi? Analizzare in che modo le tecnologie, create per liberarci, vengono invece usate per controllarci, e cercare di spostare l'asticella di un grado a favore delle persone ordinarie, invece di chi vuole avere il controllo sulle nostre vite*".

Sono queste le parole di **Edward Snowden,** il più famoso ex

agente dell'intelligence Usa, che "**La Repubblica**" ha intervistato via chat dalla **Russia**, il Paese dove Snowden risiede da 5 anni con un permesso temporaneo grazie all'appoggio del Governo.

Nato a **Elizabeth City**, negli Stati Uniti, nel 1983, Edward Snowden, ex analista della Cia ed ex collaboratore della Nsa (la National Security Agency, l'agenzia per la sicurezza nazionale Usa), è stato accusato di spionaggio a causa delle sue rivelazioni nel 2013 sui programmi top secret di sorveglianza di massa dei governi **Usa** e **Gb**.

Da quel momento per arginare il problema, Apple e altri giganti tecnologici iniziarono a blindare i propri device e le loro altre tecnologie con lo sviluppo di una crittografia molto forte, in grado di reggere la privacy degli utenti. Ma secondo Snowden, questo non è bastato ad argine lo strapotere della Nsa.

"*Se non riescono a forzare la crittografia, hackerano gli apparecchi elettronici che cifrano le nostre comunicazioni: i nostri telefoni, i nostri computer. È la via imboccata dopo il 2013 perché tanto loro hanno trovato nuove crepe per accedervi",* ha dichiarato Snowden a La Repubblica. "*Le vulnerabilità nelle tecnologie sviluppate da **Apple**, **Google** e tutte le più grandi aziende, anche **Microsoft*** – continua l'ex dipendente dell CIA nell'intervista-*, hanno una serie infinita di gravi vulnerabilità nei loro software e purtroppo non sono costrette a pagare nessuna conseguenza. Fino a quando andremo avanti così, non cambierà nulla*".

L'Italia spiata dagli Usa

Quando nel 2013 annunciò al mondo i suoi file, rivelò anche lo spionaggio Nsa contro l'Italia per influenzare le scelte

politiche del nostro Paese.

“*La ragione più importante e che non cambierà mai è semplicemente l’influenza,* continua Snowden. *“Gli Stati Uniti vogliono essere in grado di influenzare le future direzioni in cui l’Italia si muove, politicamente, economicamente e in generale. Se sei un cittadino italiano, non hai alcuna protezione legale dallo spionaggio Usa. E allora basta pensare cosa questo possa significare per un giudice italiano che indaghi su un caso che riguarda gli Stati Uniti, per un politico italiano, per un reporter che lavora a un articolo scomodo per i poteri oltreoceano*“.

https://www.key4biz.it/privacy-snowden-la-crittografia-end-to-end-non-basta-appleco-hanno-ancora-gravi-vulnerabilita/250284/

5G. Il ministro degli Esteri cinese a Bruxelles, mentre si sgonfia la campagna Usa anti-Huawei

Sul **5G** e sulla scelta delle società per la realizzazione delle reti per la tecnologia di quinta generazione la parola spetta ai singoli Stati e non all’Unione europea. A sottolineare il perimetro di competenza sul tema è stata **Federica Mogherini**, l’Alto rappresentante per la politica estera dell’Ue durante l’incontro a Bruxelles con **Wan Yi**, il ministro degli Esteri cinese.

La questione della partecipazione di Huawei alla costruzione delle reti 5G *“è competenza nazionale degli Stati membri”* e

non dell'Unione Europea, ha detto Mogherini, nella una conferenza stampa con il ministro degli Esteri cinese. *"Ne abbiamo discusso nel dialogo strategico (Ue-Cina). Lo discuteremo ulteriormente con i ministri (degli Esteri dell'Ue) a pranzo",* ha spiegato l'Alto rappresentante per la politica estera dell'Ue*. Ma "tocca agli Stati membri scegliere quali società includere o escludere dai mercati nazionali per ragioni di sicurezza",* ha concluso Mogherini.

Dunque, sono i singoli Paesi dell'Unione europea a decidere standard, regole ed aste sul 5G, per questo motivo si è rivolto direttamente agli Stati membri il ministro degli Esteri cinese, Wan Yi, chiedendo di prendere le loro decisioni in modo "*indipendente*" sulla partecipazione di Huawei alla costruzione delle reti 5G, definendo come "*immorali*" e "*senza fondamento*" le accusa lanciate dagli Stati Uniti.

Wan durante la conferenza stampa con l'Alto rappresentante per la politica estera dell'Ue ha lanciato anche un importante messaggio*: "la Cina è pronta a lavorare con i Paesi europei e con gli altri per aumentare la nostra collaborazione con la cybersecurity e trovare regole e principi universalmente accettati".*

"La Cina spera che tutti gli Stati membri creino un clima equo e giuso per accogliere le imprese di tutti i Paesi, compresi Paesi terzi. Quello che non vogliamo sono accuse senza fondamento, guidate da ragioni politiche, che hanno come unico obiettivo di distruggere imprese straniere". Queste accuse – *secondo il ministro cinese* – sono *"abnormi, immorali e non hanno il sostegno di altri Paesi. Ci auguriamo che tutti i Paesi europei saranno indipendenti nel prendere le loro decisioni"*, ha concluso Wan. Anche perché l'Ue si è munita già degli strumenti per garantire la cybersecurity: come il codice delle Tlc che regola gli investimenti nelle nuove reti, il

Cybersecurity Act e il meccanismo di screening degli investimenti esteri diretti.

Il memorandum Italia-Cina, Geraci: ‘Governo allineato su tutto dossier’

Sul memorandum Italia-Cina *“in realtà diciamo tutti la stessa cosa e siamo al 100% allineati su tutto il dossier”.* Lo sostiene il sottosegretario al ministero allo sviluppo Economico, **Michele Geraci**, a margine del Forum Italia-Cina che ha ufficialmente lanciato il progetto *Xi’An International fashion town*. *“È stato un lavoro di squadra di tutti i ministeri, non c’è stata nessuna dualità nel governo, e siamo arrivati a una sintesi ottimale perché protegge gli interessi nazionali e la sicurezza nazionale, che non va assolutamente messa in discussione, come ha ricordato Salvini”*, ha concluso Geraci.

Il presidente cinese **Xi Jinping** sarà in Europa tra il 21 al 26 marzo, ma non si conoscono i dettagli della sua visita, che lo porterà in Italia per la firma della **Nuova Via della Seta**, la “***Belt and Road Initiative***” , e andrà poi anche in Francia e Principato di Monaco. Avrà colloqui con il presidente **Sergio Mattarella** e con il primo ministro **Giuseppe Conte**. La visita del presidente Xi coincide col 50° anniversario delle relazioni diplomatiche tra Cina e Italia

Come sta andando la campagna Usa anti-Huawei con gli alleati

Nel frattempo in Europa non sta ottenendo i risultati sperati la campagna iniziata un anno fa dai funzionari americani volta a convincere gli alleati a tenere fuori Huawei dalla realizzazione delle reti 5G, nella convinzione che il colosso

di Shenzhen agisca come agente di spionaggio della Cina. Secondo il *New York Times*, infatti, la campagna Usa *"sta inciampando",* perché sta incontrando resistenze, anche fra alcuni alleati di ferro, nonostante l'avvertimento all'Europa di **Mike Pompeo**, il segretario di stato, di non concedere più agli alleati i servizi di Intelligence. Alla minaccia dell'ambasciatore americano in Germania *"di limitare l'accesso della Germania ai servizi segreti degli Stati Uniti qualora Berlino decidesse di sottoscrivere contratti con Huawei"* ha risposto, con una bella lezione di sovranità nazionale, Angela Merkel: *"Non riceviamo ordini. Definiamo da soli i nostri standard".*

Non solo la Germania, anche Gran Bretagna, India ed Emirati Arabi Uniti non credono alla accuse, senza prove, dell'amministrazione Trump. Secondo il report della National Cyber Security Uk, è possibile limitare gli eventuali rischi di spionaggio di Huawei sulla rete 5G. Un duro colpo alla campagna di geopolitica di Donald Trump. In molti sono sempre più convinti che la battaglia del presidente degli Stati Uniti non riguardi specificatamente la sicurezza nazionale degli Stati alleati, ma è il tentativo di frenare le ambizioni economiche di società della Cina. Principale competitor degli Usa nella Tech war.

Per saperne di più: 5G

> *5G. Il ministro degli Esteri cinese a Bruxelles, mentre si sgonfia la campagna Usa anti-Huawei*

Bancomat con le impronte digitali, in Uk al via i primi test

La banca britannica **NatWest** sta sperimentando l'uso di una nuova carta di pagamento **NFC** con uno scanner di impronte digitali incorporato.

Il bancomat, che sarà data solamente a 200 clienti, consentirà ai clienti di effettuare pagamenti **NFC** senza dover inserire un PIN o mettere una firma.

La cosa interessante è che non ci sono tetti massimi di spesa, normalmente nel Regno Unito (ma in Italia è uguale) non è possibile pagare via **contactless** importi superiori alle 30 sterline.

L'impronta digitale diventa quindi il modo per superare i limiti delle normali **carte NFC**. Limiti di sicurezza soprattutto, motivo per cui quasi tutte le carte di questo tipo possono essere usate in questo modo solo per spese modiche.

I dati relativi alle impronte digitali sono memorizzati localmente sulla carta, il che significa che non ci sono informazioni di sicurezza che un hacker possa rubare dal database centrale di una banca.

Certo, questo sistema non è infallibile: c'è sempre il rischio che un ladro possa rubare e 'copiare' la tua impronta digitale, ma è molto più sicuro di un codice PIN.

L'autenticazione biometrica è diventata una componente standard dei pagamenti mobili NFC, ma nonostante siano state

già condotte delle prove non sono riusciti ancora a trovare l'utilizzo nelle banche tradizionali.

Gemalto, la società che ha sviluppato la tecnologia biometrica della carta, l'anno scorso l'aveva già sperimentato con la banca italiana **Intesa Sanpaolo.**

Bancomat con le impronte digitali, in Uk al via i primi test

Cloud e cybersecurity, Cuneo prima tappa del roadshow di CSI Piemonte

Ogni giorno il **CSI Piemonte** protegge la pubblica amministrazione piemontese da **circa 150.000 attacchi informatici**. Si tratta di un numero significativo, che testimonia dell'importanza sempre più crescente di temi come **sicurezza informatica**, **protezione dei dati personali** e **servizi in cloud**. E proprio questi sono i concetti che vengono affrontati dal **roadshow "Territori del futuro. Cloud e sicurezza, la trasformazione digitale parte da qui"**, che ieri ha fatto **tappa a Cuneo**, presso la sede della Camera di Commercio.

L'evento è stato organizzato da **CSI Piemonte**, **Regione Piemonte** e **Fondazione Torino Wireless** per condividere esigenze, esperienze e buone pratiche con amministratori pubblici e imprese, e per fare il punto sulle opportunità disponibili e confrontarsi sulle strategie future nel settore ICT.

Aperto dai saluti dell'Assessore regionale all'Innovazione

Giuseppina De Santis, del Direttore Generale del CSI **Pietro Pacini** e del Vice Presidente Esecutivo di Torino Wireless **Mario Manzo**, l'incontro ha visto la partecipazione fra gli altri di **Marco Bussone** (Presidente UNCEM), di **Michele Pianetta** (Vice Presidente ANCI Piemonte), di **Giandomenico Genta** (Presidente Fondazione Cassa di Risparmio di Cuneo), di **Pier Angelo Mariani** (Comune di Cuneo), di **Alessandro Risso** (Provincia di Cuneo) e **Luca Brusutti** (Infocamere).

Al centro dei lavori l'offerta di servizi pubblici al cittadino, che oggi è sempre più digitale e per questo si espone inevitabilmente ai rischi legati alla **vulnerabilità dei sistemi** e al fenomeno della **criminalità cyber**. La necessità di analizzare questi rischi e mettere in sicurezza dati, servizi e informazioni assume quindi un ruolo più che mai cruciale per la Pubblica Amministrazione. Ma qual è il livello di consapevolezza degli Enti e delle Aziende del territorio su questo tema? Quali sono le strategie messe in atto per prevenire gli attacchi informatici e proteggere i dati in un mercato in continua evoluzione?

"*Noi possiamo aiutare il territorio e tutte le sue amministrazioni a far fronte a questi pericoli*", ha spiegato **Pietro Pacini**. "*Il CSI può infatti mettere a disposizione l'esperienza del proprio Security Operation Center, un centro specializzato in sicurezza informatica in grado di fornire attività di formazione, supporto progettuale e organizzativo e di erogare servizi di sicurezza specifici. Con l'obiettivo di fare "rete" sul territorio per diffondere e applicare i principi della sicurezza informatica*".

"*Siamo qui oggi a Cuneo ospiti della Camera di Commercio per condividere quanto stiamo facendo e abbiamo già fatto su temi chiave come la sicurezza informatica e il cloud*", ha affermato **Giuseppina De Santis**. "*Per questo sono lieta che CSI Piemonte*

e Fondazione Torino Wireless abbiano rafforzato la loro collaborazione e dato vita a questo ciclo di incontri, visto che si tratta di due realtà che operano in modo complementare proprio verso gli enti pubblici e le aziende. Da un lato, infatti, il CSI si muove oggi come partner strategico della pubblica amministrazione a vantaggio non solo della Regione ma di tutto territorio, mentre TorinoWireless lavora a favore delle imprese ed è soggetto attuatore del cluster nazionale per le smart communities. Il nostro obiettivo comune è quello di realizzare servizi che siano utili e usabili da tutti: enti, PMI, cittadini e famiglie. E che possano popolare in modo sempre più efficace l'infrastruttura di rete BUL (Banda Ultra Larga) che stiamo realizzando".

Per **Mario Manzo** – Vice Presidente Esecutivo di Torino Wireless "*L'osservatorio Agenda Digitale del Politecnico di Milano del 2018 ha evidenziato come nonostante i passi avanti fatti nell'ultimo anno nei processi di digitalizzazione delle pubbliche amministrazioni locali, molto resti ancora da fare in ottica di "switch off" di servizi pubblici, dove esistono ancora ritardi importanti. Nel 2018 solo il 21% dei comuni intervistati dall'Osservatorio ha smesso di erogare in modalità tradizionale ripensandone la gestione esclusivamente attraverso canali digitali. Un ulteriore 21% ha in cantiere progetti di switch-off per il 2019, mentre oltre il 65% dei Comuni non ha ancora fatto né intende attivare iniziative a breve. La messa a fattore comune di asset e di competenze di enti strumentali come il CSI, Infocamere e la Fondazione Torino Wireless, può aiutare le pubbliche amministrazioni locali ad essere messe nelle condizioni di offrire servizi con modalità più moderne e inclusive, digitalizzando i processi, migrando verso infrastrutture tecnologiche più moderne, gestendo la cybersecurity e i big data della PA, tutelando adeguatamente la privacy del cittadino, aumentandone la soddisfazione, ed ottenendo conseguenti risparmi diretti di spesa e maggiori entrate e risorse liberate per nuovi investimenti. Dobbiamo solo continuare a lavorare tutti*

insieme valorizzando le buone pratiche delle nostre imprese, utilizzando gli strumenti regionali messi a disposizione e, soprattutto, investendo in formazione e awareness"

"*Per il ruolo che la Fondazione riveste, a livello provinciale e nazionale, e per l'importanza dei dati che costudiamo, il nostro ente è da sempre molto attento al tema della sicurezza informatica*" ha aggiunto **Giandomenico Genta**, Presidente della Fondazione CRC. "*In parallelo, promuoviamo e sosteniamo numerosi progetti che mirano a garantire l'innovazione e l'infrastrutturazione tecnologica del nostro territorio, elementi strategici per uno sviluppo smart, sostenibile e inclusivo*".

L'altro grande fronte di riorganizzazione per la pubblica amministrazione riguarda invece **l'adozione di infrastrutture cloud**, che consentono di migliorare la sicurezza, la protezione dei dati e l'efficienza dei sistemi ICT. Il cloud permette di ridurre i costi, rendere più semplice ed economico l'aggiornamento dei software e di velocizzare l'erogazione dei servizi a cittadini e imprese. Il Piano Triennale sull'Informatica nella PA e le successive circolari emesse dall'AgiD, l'Agenzia per l'Italia Digitale, hanno infatti individuato nel cloud un potente strumento di ammodernamento della macchina amministrativa e di trasformazione digitale.

"*Grazie all'esperienza maturata negli ultimi anni e al recente riconoscimento come Cloud Service Provider qualificato* – ha proseguito **Pacini** – *il CSI Piemonte è in grado di affiancare le PA e le imprese in questo percorso mettendo a disposizione i propri data center, la propria piattaforma certificata ed elevate competenze tecniche, progettuali e organizzative.*

"*Anche le Camere di commercio ricoprono una funzione fondamentale in questo processo di trasformazione digitale* – ha evidenziato il **Presidente Ferruccio Dardanello**. *Grazie ai Pid – Punti di impresa digitale – attivati su tutto il territorio, ai nuovi servizi sempre più digitali offerti per*

il tramite della propria società informatica Infocamere, all'organizzazione di eventi formativi e divulgativi, agli strumenti di valutazione del grado di digitalizzazione e ai voucher di sostegno economico al digitale, gli enti camerali intendono affermare il nuovo ruolo a sostegno della trasformazione digitale delle imprese del territorio per favorire, in sinergia con gli altri soggetti pubblici e privati, il salto tecnologico oggi indispensabile alla competizione sui mercati nazionali e internazionali".

Gli appuntamenti del roadshow "Territori del futuro. Cloud e sicurezza, la trasformazione digitale parte da qui" non si fermano qui. Prossima tappa a Biella, il 28 marzo.

Per saperne di più: Cloud

Cloud e cybersecurity, Cuneo prima tappa del roadshow di CSI Piemonte