Samsung WOW Business Summit 2017: la cybersecurity è una priorità alla base dello sviluppo economico nazionale. L'impegno parte dalla messa in sicurezza degli smartphone e degli oggetti connessi

La terza edizione dell'annuale Business Summit di Samsung, ha affrontato uno dei temi chiave per un mondo nel quale la pervasività del digitale rende sempre più necessarie soluzioni di sicurezza per le imprese e per i singoli cittadini

Milano, 26 ottobre 2017 – La **cybersecurity** è la **seconda emergenza in Europa**, dopo il cambiamento climatico e prima dell'immigrazione, come emerge dall'ultimo meeting sullo stato dell'Unione Europea dello scorso 13 settembre; **tutte le grandi aziende e le infrastrutture critiche nazionali subiscono ogni giorno attacchi informatici** e nel solo **2016 il 47% delle aziende piccole e medie in Italia ha subito almeno un attacco** (fonte: Banca d'Italia). Questo dato subirà di sicuro un **forte incremento nel 2017**, a causa delle ultime **campagne malware** ("wannacry" e "notpetya") che hanno messo fortemente a rischio la sicurezza di intere aziende le quali, secondo alcuni dati recenti, hanno un **costo medio di 3,5 milioni di euro per ogni attacco andato a buon fine**, mentre per le **piccole e medie imprese gli attacchi informatici possono mettere a repentaglio l'esistenza della azienda stessa**.

Non è un caso che l'Europa stessa si sia mossa per sollecitare i lavori **dell'Agenzia Europea per la sicurezza delle reti e dell'informazione** (Enisa), affinché strutturi un **piano di intervento comune**, adotti un'etichetta che certifichi la sicurezza dei dispositivi connessi, e persino crei un fondo di solidarietà a sostegno dei Paesi che dovessero trovarsi in difficoltà a causa di un attacco informatico su vasta scala.
Assodato che per **la sicurezza informatica non esiste una ricetta unica in grado di fronteggiare qualsiasi attacco**, esistono altresì alcuni ingredienti fondamentali sui quali il sistema paese è chiamato a concentrarsi per alzare le difese.
In questo contesto, il crescente tema della **mobilità**, la sempre maggiore diffusione del **BYOD** (bring your own device), la crescita dell'**IoT** (Internet of Things) sono tutti elementi presi in considerazione nella definizione di uno scenario di lotta agli attacchi informatici. i **dispositivi intelligenti connessi alla rete** (ambito IoT) **potenzialmente hackerabili** saranno **oltre 100 miliardi di cui almeno 1 miliardo in Italia**; mentre una recente ricerca portata avanti negli Stati Uniti (BYOD and Mobile Security Report - September 2016), fa emergere che **il 20% degli incidenti di sicurezza informatica avvenuti nelle grandi aziende ha coinvolto uno smartphone**.

Da queste considerazioni relative alla necessità di creare un circolo virtuoso di informazioni atte a fronteggiare le minacce della cybersecurity e dalla necessità di evidenziare gli elementi che possono concorrere alla difesa del sistema Paese nel complesso, ha preso il via la terza edizione di "**WOW - Wide Opportunities World**" (presso il The Mall a Milano), il Business Summit organizzato ogni anno da Samsung, durante il quale **esponenti di spicco della pubblica amministrazione e delle principali aziende italiane** si sono incontrati per un confronto sulle tematiche più rilevanti del mondo imprenditoriale, e per fornire strumenti e prospettive volte a sviluppare il business in chiave digitale.

Samsung WOW Business Summit 2017: i risultati della discussione

La **sicurezza informatica** è certamente **centrale non solo nel dibattito sullo sviluppo del digitale nel nostro Paese e nel mondo**, ma anche **per lo sviluppo stesso dell'economia in tutti i suoi aspetti**. I relatori che hanno preso parte al dibattito di oggi al Samsung Business Summit, aperto dai saluti di **Roberta Cocco**, Assessore alla Trasformazione Digitale e Servizi Civici del Comune di Milano, si sono posti l'obiettivo di **supportare le aziende e la società civile ad affrontare le complessità di un tema sempre più caldo**, e **facilitare la condivisione delle informazioni sui rischi e le soluzioni adottabili per reagire alle minacce informatiche con la forza di una solida comunità di business**.
Dal confronto è emersa **la volontà di creare una collaborazione sempre più stretta e fruttuosa tra i soggetti chiamati da un lato a muoversi in un mercato molto competitivo e sempre più strategico per il sistema imprenditoriale**, e dall'altro ad **essere sempre pronti ad affrontare i pericoli che hanno spazzato via l'idea stessa di invulnerabilità** e che **costringono ad allargare il concetto stesso di difesa ben al di là del perimetro della propria azienda**.

"L'evoluzione digitale è oggi un grande traguardo, ma la digital transformation senza la sicurezza è nulla, in quanto espone il proprio business al rischio di attacchi esterni. E non ci sarà una crescita del digitale se non ci saranno le premesse per sentirsi sicuri nell'affrontare il cambiamento imposto dalle nuove tecnologie", ha

affermato **Carlo Barlocco**, Presidente di Samsung Electronics Italia. *“Il nostro Paese ha ancora molte opportunità da cogliere nel digitale per indirizzare la crescita economica e favorire il benessere dei cittadini, ma in questo ambito è fondamentale riuscire a fare fronte comune tra la politica, la società civile e il mondo aziendale. E Samsung, da sempre attenta ai temi della sicurezza con particolare attenzione alla sfera della mobilità, dell’IoT, dei pagamenti digitali e dello smart working, cerca di ricoprire il ruolo di facilitatore che accompagna le aziende in questo viaggio, per aumentarne la produttività”.*

Subito dopo il saluto del Presidente di Samsung Italia, il summit ha affrontato subito le priorità per l’Italia in tema di sicurezza dei dati, con l’intervento del Professore **Roberto Baldoni**, Direttore CIS Sapienza Università di Roma e Direttore Laboratorio Nazionale di Cybersecurity (CINI), il quale ha subito evidenziato la natura di emergenza assunta dalla cybersecurity in Europa e la necessità di mettere il tema al centro delle politiche di trasformazione digitale per non mettere a serio rischio la propria prosperità economica. Una delle azioni più importanti nel settore privato - ha detto Baldoni - è stata la realizzazione del Framework Nazionale per la cybersecurity, un manuale orientato alle aziende per una corretta gestione del rischio cyber, nato da una Public Private Partnership che includeva il CERT Nazionale, il Garante della Privacy, la Presidenza del Consiglio dei Ministri, e alcune aziende nazionali strategiche come ENEL e ENI. Il tutto guidato dal centro di ricerca CIS Sapienza e dal Laboratorio Nazionale di Cybersecurity che include quaranta università pubbliche e private e diversi centri di ricerca nazionali. Il Framework nazionale di cybersecurity ha introdotto l'importanza di una corretta gestione del rischio all'interno di una azienda partendo dal consiglio di amministrazione e dal comitato rischi. In seguito al framework sono stati pubblicati quest'anno i controlli essenziali per la cybersecurity, una versione semplificata del framework, orientata alle piccolissime, piccole e medie imprese.

Successivamente all’intervento di Baldoni, la giornata ha visto l’alternarsi di **due panel dedicati rispettivamente agli aspetti legati ai progetti e agli investimenti delle aziende italiane e al rapporto fra istituzioni e cybersecurity, per fare il punto sulla sicurezza del Paese**.

Al **primo panel** hanno preso parte: **Andrea Malacrida**, Amministratore Delegato The Adecco Group Italia; **Fabio Cappelli**, **Fabio Cappelli**, Partner EY, Mediterranean Cyber security Leader; **Simone Puksic**, Presidente del Consiglio di Amministrazione di Insiel S.p.A e Presidente di Assinter Italia; **Roberto Baldoni**, Direttore CIS Sapienza Università di Roma e Direttore Laboratorio Nazionale di Cybersecurity (CINI); **Giorgio Mosca**, Presidente Cybersecurity Steering Committee Confindustria Digitale; **Francesco Morelli**, Responsabile della Tutela Aziendale di Terna S.p.A.

Protagonisti del **secondo panel** sono stati: l’onorevole **Sergio Boccadutri**, Membro dell’Intergruppo Parlamentare Innovazione e Responsabile Innovazione PD; **Guido Bortoni**, Presidente Authority per l’Energia; **Riccardo Capecchi**, Segretario Generale AGCOM; **Maurizio Pimpinella**, Presidente dell’Associazione Italiana Prestatori di Servizi di Pagamento (APSP); **Andrea Raffaelli**, Tenente Colonnello, Comandante Carabinieri ROS (Reparto Operativo Speciale); **Salvatore La Barbera**,
Primo Dirigente, Polizia Postale di Milano.

Tra le indicazioni emerse durante il dibattito, i diversi relatori hanno sottolineato i seguenti punti:

“*Le forme di digitalizzazione impongono già oggi e sempre più imporranno domani la capacità di gestire, immagazzinare e interpretare enormi quantità di dati. Per noi di The Adecco Group, che gestiamo la vita professionale di migliaia di persone, la sicurezza di questi dati è e deve essere una priorità strategica, alla quale destiniamo risorse professionali ed economiche considerevoli. Da un altro punto di vista la digitalizzazione e le nuove policy di sicurezza legate alle organizzazioni sono sempre più destinate a divenire data centriche, porteranno alla creazione di nuove professioni e professionalità, creando miglia di nuove opportunità nel mondo del lavoro*.” - **Andrea Malacrida**, Country Manager, Adecco

"La protezione digitale non consiste più solo nella sicurezza delle informazioni, ma coinvolge la difesa delle persone e dei processi aziendali. In un mondo dove 50 miliardi di dispositivi saranno connessi entro il 2020 in un’unica rete globale e dove una nuova tecnologia impiega 35 giorni per raggiungere una massa critica di 50 milioni di utenti, la cyber security gioca un ruolo fondamentale nel garantire la fiducia nel nuovo ecosistema digitale ed il successo dei nuovi modelli innovativi" **Fabio Cappelli**, Partner EY, Mediterranean Cyber security Leader

“Oggi la PA deve cogliere le opportunità del digitale e dell’economia della conoscenza: i dati saranno il più grande patrimonio dell’umanità post industriale! Per questo è necessario processarli e proteggerli con tecnologie e metodi agili.” - **Simone Puksic**, Presidente del Consiglio di Amministrazione di Insiel S.p.A; Presidente di Assinter Italia

“La sicurezza digitale sta diventando uno dei principali temi a cui la società nel suo insieme deve porre attenzione. La Commissione Europea propone una nuova strategia continentale, il Governo italiano promuove un riassetto delle attività nazionali, Confindustria opera per la sicurezza della nuova filiera digitale abilitata dal Piano Industria 4.0. Non sono iniziative distinte: non c’è sicurezza se non agiamo come sistema.” **Giorgio Mosca**, Presidente, Cybersecurity Steering Committee Confindustria Digitale

“Per ottenere dei risultati è fondamentale un'attività interna di cyber security awareness volta a migliorare la consapevolezza delle minacce e delle vulnerabilità nei diversi utenti dei sistemi critici, contribuendo ad aumentare in loro il rispetto delle politiche di sicurezza e a migliorare la loro condotta nelle eventuali situazioni di emergenza.” - **Francesco Morelli**, Responsabile della Tutela Aziendale di Terna S.p.A.

“È necessario ridurre la vulnerabilità informatica delle Pubbliche Amministrazioni, perché custodiscono i dati di 60 milioni di italiani.” On. **Sergio Boccadutri**, Membro dell’Intergruppo Parlamentare Innovazione e Responsabile Innovazione PD

“L’attenzione alla cybersecurity nell'energia è un effetto dell'auspicata decentralizzazione di generazione, di domanda attiva e di accumulo” **Guido Bortoni**, Presidente Authority per l’Energia

“Garantire la sicurezza delle reti e di chi vi opera significa leggere e regolare in modo convergente i profili “hard”, intesi come caratteristiche tecniche delle infrastrutture e dall’altro la dimensione “soft”, ovvero quella delle tutele e dei diritti di chi immette in rete i propri contenuti, sia di natura individuale che d’impresa.” - **Riccardo Capecchi**, Segretario Generale, AGCOM

“I cittadini devono imparare a usare i nuovi pagamenti digitali in modo più consapevole e sicuro: per questo è oggi necessaria un’azione formativa ed educativa. Gli smartphone sono anche facili punti di accesso a password e dati personali e, spesso, non si è consapevoli delle informazioni che si mettono a disposizione degli algoritmi degli Over The Top. Bisogna, inoltre, imparare a difendersi dai tentativi di frode diventati oggi più sofisticati.” - **Maurizio Pimpinella**, Presidente dell’Associazione Italiana Prestatori di Servizi di Pagamento (APSP)

“Cybersecurity e Cybercrime sono due facce della stessa medaglia e vanno studiate, analizzate e gestite insieme per ottenere un risultato ottimale” - **Andrea Raffaelli**, Tenente Colonnello, Comandante Carabinieri ROS (Reparto Operativo Speciale)

Nello stesso contesto del Business Summit, Samsung ha fatto emergere i risultati di un **sondaggio relativo alla percezione e ai livelli di protezione e sicurezza dei device nell’ambito personale e lavorativo**, basato sulle risposte degli **oltre 500 partecipanti** provenienti dalle aziende italiane e straniere, di diversi settori industriali (siderurgia, servizi, finance, banking, consulenza, tecnologia etc.) che hanno aderito all’evento.
Tra i principali dati della ricerca emerge che:

- Il **35,7%** degli intervistati ritiene che il proprio smartphone sia in generale poco sicuro e che qualcuno possa accedere alle informazioni personali; il **33,4%** ritiene invece il proprio smartphone abbastanza sicuro a fronte di accessi esterni; **il 26,5%** ritiene lo smartphone molto sicuro e che nessuno possa violare la privacy dei dati personali; solo il **4,4%** ritiene il proprio dispositivo mobile per niente sicuro e accessibile da chiunque all’esterno
- Il **50,7%** dei partecipanti alla survey ritiene che i file contenuti sul proprio smartphone (immagini, video, documenti etc.) siano solo parzialmente al sicuro e che i metodi di protezione adottati non siano del tutto affidabili; il **30,9%** invece pensa che siano al sicuro e non possano essere violati da persone non autorizzate; mentre il **18,4%** è convinto che siano insicuri e chiunque potrebbe accedervi in qualsiasi momento
- Addirittura il **93,2%** dei rispondenti ritiene che le proprie ricerche su internet dallo smartphone siano normalmente rintracciabili da soggetti terzi; solo l’**1,5%** pensa che non sia possibile accedere alle proprie ricerche; il restante **5,3%** dimostra di non avere sensibilità in materia
- Quale è invece il livello di percezione in relazione alla sicurezza in ufficio? In questo caso gli utenti aziendali si sentono più rassicurati: infatti l’**87,1%** degli intervistati ritiene che il proprio luogo di lavoro metta a disposizione degli strumenti di difesa dagli attacchi informatici; solo il **6,7%** non si sente al sicuro, mentre un altro **6,2%** non è a conoscenza di eventuali sistemi di protezione all’interno della propria azienda;
- La platea risulta abbastanza spaccata rispetto ai provvedimenti in tema di sicurezza informatica intrapresi dal governo italiano: infatti, il **39,8%** li ritiene al momento adeguati, il **33%** pensa invece

che non sia adeguati, mentre il restante **27,2%** non ha una visione ben chiara di come l'amministrazione pubblica in Italia si stia muovendo in tema di cybersecurity.

Samsung Electronics
Samsung ispira il mondo e delinea il futuro attraverso idee e tecnologie rivoluzionarie, trasformando il mondo dei TV, smartphone, tecnologie indossabili, tablet, elettrodomestici, sistemi di rete e memorie, sistemi LSI e soluzioni LED. Per essere aggiornati sulle ultime novità, è possibile visitare la sezione Samsung Newsroom su www.samsung.com.

Samsung Electronics Italia
Viale Mike Bongiorno, 9 - 20124 Milano
Tel. +39 02 921891
Laura di Bari l.dibari@samsung.com
Manuele De Mattia m.demattia@samsung.com

Ufficio Stampa
Edelman Italy - Ufficio Stampa Samsung
Livio Tarallo: livio.tarallo@edelman.com (+39) 02 63116285

Samsung – La protezione dei dispositivi mobile in 10 punti

A margine del Summit, Samsung ha anche condiviso con il pubblico un utile **vademecum** rivolto ai consumatori finali, che espone in maniera semplice e diretta i **10 punti base per la messa in sicurezza dei dispositivi mobile**; i punti del vademecum saranno declinati nei prossimi mesi sui canali online e social dell'azienda.

1. **Mantenere il dispositivo mobile sempre aggiornato**
   Bisogna ricordarsi sempre di **aggiornare il sistema operativo e gli altri software che si utilizzano**: gli aggiornamenti spesso includono patch contro vulnerabilità e minacce alla sicurezza che potrebbero essere utilizzate e sfruttate contro l'utente.
   Sui dispositivi Samsung: durante la vita del dispositivo mobile, Samsung rilascia aggiornamenti software ed aggiornamenti dei criteri di protezione di Samsung Knox. Questo è assolutamente normale e garantisce la perfetta funzionalità del prodotto nel tempo. Per questo motivo è importante verificare dal menu Impostazioni la disponibilità degli aggiornamenti rilasciati periodicamente da Samsung ed effettuarne l'installazione. Non installare versioni software non sviluppate da Samsung e non effettuare il root (dall'inglese "radice") del dispositivo perché, oltreché a invalidare la garanzia del prodotto, riduce enormemente la sua sicurezza.

2. **Attivare l'antivirus**
   Prevenire è meglio che curare… Utilizzare una soluzione di sicurezza (antivirus) che protegga i dati ai quali si tiene di più.
   Sui dispositivi Samsung: I terminali Samsung più recenti integrano un software antivirus. E' bene assicurarsi di attivarlo dal menù Impostazioni.

3. **Impostare una tipologia di blocco dello schermo**
   Questo semplice gesto rappresenta la prima linea di difesa contro l'accesso ai nostri dati personali in caso di tentativo da parte di terzi di accedere al dispositivo, ad esempio in caso di smarrimento o furto. L'impostazione base prevede l'impostazione di una password alfanumerica o di un PIN.
   Sui dispositivi Samsung: Oltre alle comuni password/PIN e segno, disponibili su tutti gli smartphone, sui dispositivi Samsung più recenti è possibile impostare lo sblocco dello schermo tramite impronta digitale oppure attraverso la lettura dell'iride. Queste due modalità abilitano un livello di protezione ancora più elevato e al tempo stesso estremamente immediato.

4. **Attivare il PIN di blocco della SIM**
   Molto spesso ci si preoccupa di proteggere il proprio smartphone ma ci si dimentica di impostare un blocco a livello di scheda SIM. E' consigliabile attivare anche il blocco SIM, per garantire anche la massima protezione della scheda stessa e dei dati che contiene.

5. **Installare la applicazioni solo dagli Store ufficiali**
   E' consigliabile installare software proveniente solo da fonti attendibili. Gli store ufficiali quali Google

Play Store, Apple App Store e Samsung Galaxy Apps sono la scelta più sicura ed offrono maggior protezione rispetto ad applicazioni provenienti da sorgenti non ufficiali. Inoltre, è buona norma impostare il proprio dispositivo affinché, nel menu Impostazioni, l'installazione da sorgenti sconosciute sia disabilitata.
E' buona cosa verificare anche che l'applicazione che si sta installando sia quella che effettivamente l'utente desidera usare, evitando di installare quelle che hanno semplicemente nomi o logo simili, spesso creati appositamente per trarre in inganno.

6. **Verificare le autorizzazioni concesse alle applicazioni**
Quando si installa o si utilizza una nuova applicazione, bisogna prestare attenzione alle informazioni alle quali l'applicazione vuole accedere. E' bene prestare attenzione ai messaggi in cui viene richiesto di autorizzare l'app ad accedere a contenuti del dispositivo; leggerli con cura è un buon modo per verificare che l'applicazione che si sta installando non acceda in maniera inopportuna, e per altri fini, ai propri dati personali.

7. **Prestare attenzione quando si forniscono informazioni personali**
Il phishing è un tipo di truffa attraverso la quale un malintenzionato cerca di ingannare la vittima convincendola a fornire informazioni personali, codici di accesso, dati della carta di credito o del conto corrente, fingendosi un ente affidabile in una comunicazione digitale. Normalmente il phishing ha l'aspetto di una email che invita l'utente a cliccare un link e ad inserire i propri dati.
E' fortemente consigliato cancellare tutte le email sospette che si ricevono, specialmente se includono link o allegati. Se si pensa che il messaggio provenga veramente dal mittente indicato, è utile verificare direttamente con il mittente, o con l'azienda per la quale lavora, nel caso in cui l'email provenga da un mittente aziendale.

8. **Abilitare la cifratura dei dati**
I terminali più recenti abilitano la crittografia dei dati di default; inoltre consentono di proteggere ulteriormente i propri dati in caso di furto o smarrimento attraverso una password che viene richiesta solo all'accensione.
Sui dispositivi Samsung: questa funzione è denominata Avvio Protetto ed è disponibile nel menu Impostazioni. Bisogna ricordare che la crittografia dei dati sulla scheda SD non è di default e va impostata dall'utente per proteggere anche i dati sulla scheda esterna.

9. **Abilitare il controllo remoto del proprio dispositivo in caso di smarrimento o furto**
Avere la possibilità di geolocalizzare oppure bloccare il proprio telefono a distanza è importante per proteggere i dati personali in caso di smarrimento o furto.
Sui dispositivi Samsung: Samsung mette a disposizione il servizio integrato "Find my Mobile" che permette una gestione puntuale del proprio dispositivo anche quando si trova lontano da noi. E' bene assicurarsi di aver configurato un Samsung Account sul proprio dispositivo ed aver abilitato la funzionalità dal menu Impostazioni. L'accesso al servizio Find my Mobile è possibile da qualunque browser accedendo al link https://findmymobile.samsung.com

10. **Ripristinare il dispositivo prima di rivenderlo**
Se si ha l'intenzione di acquistare un nuovo dispositivo mobile e rivendere l'attuale come usato, bisogna assicurarsi di ripristinarlo alle condizioni di fabbrica. Il consiglio è quello di verificare che la cifratura sia attiva prima di eseguire la cancellazione dei dati, cosi che non rimangano informazioni e contenuti personali al suo interno.