RASSEGNA STAMPA

Lanci agenzia per ITASEC 2018

Itasec18: senza cybersecurity a rischio sviluppo del Paese

(AGI) - Roma, 5 feb. - Senza una gestione nazionale della sicurezza informatica, le minacce saranno "difficile da contenere" e avranno "conseguenze rilevanti sull'indipendenza e sullo sviluppo del Paese". Lo afferma il libro bianco "Il futuro della cybersecurity in Italia: Ambiti Progettuali Strategici". Il documento sara' presentato il 6 febbraio, nel corso di Itasec18, seconda conferenza nazionale sulla sicurezza informatica organizzata dal Laboratorio Nazionale di Cybersecurity del Cini. I curatori (Roberto Baldoni, oggi vicedirettore generale del Dis con delega alla cybersecurity, Rocco De Nicola dell'Imt di Lucca, e Paolo Prinetto del Politecnico di Torino) scattano una fotografia delle sfide che la digitalizzazione impone. E indicano alcune raccomandazioni. "La difesa - afferma Paolo Prinetto, presidente del Cini - deve essere basata sulla condivisione delle informazioni e sulla massima velocita di risposta. Nel 2016 il cybercrime e costato all'economia mondiale qualcosa come 450 miliardi di dollari, piu' o meno quanto il Pil dell'Austria. Secondo dati della Banca d'Italia, il 45,2% delle aziende italiane ha subito un attacco tra il settembre 2015 e il settembre 2016 e la percentuale sale al 62,8 % nel caso di aziende con piu di 500 addetti". Oggi, sottolinea il documento, "mancano servizi che, su scala nazionale, consentirebbero di sorvegliare con continuita particolari porzioni di Internet considerate critiche (legate a energia, trasporti, servizi finanziari, informazione)". (AGI) Di2/Ila (Segue)

Itasec18: senza cybersecurity a rischio sviluppo del Paese (2)

(AGI) - Roma, 5 feb. - Le espressioni piu' popolari di attacchi informatici sono i ramsonware, come wannacry e notpetya, il phishing e le fake news (che per il libro bianco sono una cyber-minaccia). Ma si tratta solo "della punta di un iceberg che, nelle parte sommersa, e' costituito da migliaia di campagne giornaliere". Le tecniche di attacco, sempre piu' sofisticate, portano spesso le vittime ad accorgersi troppo tardi di aver subito un danno. "La correzione di una vulnerabilita - spiega il libro bianco - puo impedire che venga sfruttata nuovamente, ma non puo fare nulla nei confronti dell'attacco che l'ha portata alla luce. E necessario quindi un approccio proattivo di cosiddetta difesa attiva". Cioe' di prevenzione. Azzerare i pericoli e' impossibile. Ma una politica corretta di cybersecurity nazionale puo' rendere i rischio "accettabile nel tempo". Come? Innanzitutto il libro bianco, oltre a sollecitare il rafforzamento di strutture esistenti (come il Nucleo Sicurezza Cibernetica), propone la creazione di centri dedicati alla cybersecurity, distribuiti sul territorio ma che facciano capo a una regia unica: un Centro Nazionale di Ricerca e Sviluppo in Cybersecurity; i Centri Territoriali di Competenza; Centri Verticali dedicati a settori di mercato specifici. Sarebbe poi utile battezzare una fondazione. Tra i suoi compiti ci sarebbe la promozione di una "Cybersecurity Academy", descritta come un "conservatorio musicale" della sicurezza informatica: un istituto che possa seguire nel tempo la crescita dei talenti. E poi ci sarebbe "un fondo di venture capital etico per la creazione e il rafforzamento di start-up che sviluppino tecnologia di interesse nazionale". Sarebbe un incentivo perche' consentirebbe ai risultati di ricerca accademica di "trasformino in opportunita di business". Il Cini chiede che la cybersecurity diventi centrale, che venga considerata "parte integrante della politica digitale nazionale" e che ricada sotto la

responsabilita' diretta del Presidente del Consiglio. Al capo del governo, i curatori del documento chiedono di creare un comitato di esperti per la trasformazione digitale e un Centro di Valutazione e Certificazione Nazionale: servirebbe a identificare e verificare software e hardware sicuri (da usare nella Pa). Gia' adesso, e ancora di piu' nel prossimo futuro, i Paesi concorreranno per aggiudicarsi i talenti migliori. Serve quindi coltivarli, ma anche saperli trattenere e attrarre. (AGI) Di2/Ila (Segue)

Itasec18: senza cybersecurity a rischio sviluppo del Paese (3)

(AGI) - Roma, 5 feb. - In Gran Bretagna sono stati investiti piu di 20 milioni di euro nel Cyber Schools Programme destinato ai giovani tra i 14 e i 18 anni, per incoraggiarli a occuparsi di sicurezza informatica. In Italia, al momento, nelle scuole superiori viene dato poco spazio alla cybersecurity e, "tra le 34 azioni considerate nel Piano Nazionale per La buona Scuola digitale, non figura alcuna azione dedicata alla cybersecurity". I talenti, invece, andrebbero cercati: "La sfida principale - si legge nel libro bianco - e quella di intercettarli in una fase del loro percorso di studi in cui non abbiano ancora deciso una direzione definita su cui investire le proprie capacita, presentando loro le possibilita di carriera e gli aspetti stimolanti delle attivita in cybersecurity". Anche attraverso "la partecipazione femminile, sfatando il principio per cui la cybersecurity e un dominio per soli uomini". Nelle scuole e nelle universita', pero', mancano persone con una formazione specifica: "In questo momento il loro numero e cosi basso che le Universita non riescono ad attivare, in autonomia, programmi di ricerca o di didattica. E' necessario un piano straordinario per l'assunzione di ricercatori e professori universitari del settore". Oltre a questi programmi, sottolineano Baldoni, De Nicola e Prinetto, "dobbiamo creare le condizioni per riportare in Italia i nostri migliori cervelli". La cybersecurity pero' non puo' essere imposta per legge. Anche gli utenti finali devono conoscere le regole base: "Molte volte i danni di attacchi informatici dipendono da un anello debole identificabile: il fattore umano. Un click sbagliato puo infatti distruggere qualsiasi linea di difesa tecnologica di un singolo apparato, di una organizzazione, di un Paese. Sono le persone che si fanno 'pescare' da una campagna di phishing, che usano come password il nome del gatto o del consorte, che usano lo stesso smartphone per farci giocare i figli e poi accedere alla rete aziendale". (AGI)

Cybersecurity: Itasec18, blockchain possibile rivoluzione

(AGI) - Roma, 6 feb. - "La blockchain potrebbe essere una vera rivoluzione perche' non protegge solo il dato ma anche la sua storia". Lo ha affermato Rocco De Nicola, professore dell'Imt di Lucca, intervenuto nel corso di Itasec18 per presentare il libro bianco 'Il futuro della cybersecurity in Italia: Ambiti Progettuali Strategici'. "Come nazione dobbiamo stare attenti a questo fenomeno. Potrebbe essere una bolla, ma dobbiamo prepararci al fatto che non lo sia". Non approfondire la blockchain potrebbe avere "effetti dirompenti". (AGI)

Cybersecurity: Itasec18, cautela per il voto digitale

(AGI) - Roma, 6 feb. - Serve "grande cautela nell'e-voting" cioe' nei sistemi di voto digitali. Lo ha affermato Rocco De Nicola, professore dell'Imt di Lucca, intervenuto nel corso di Itasec18 per presentare il libro bianco "Il futuro della cybersecurity in Italia: Ambiti Progettuali Strategici". "La

forza dell'attacco - ha sottolineato - dipende dalla possibile ricompensa. E il controllo di uno Stato mi sembra abbastanza ricca". De Nicola ha indicato la necessita' di una maggiore collaborazione tra istituzioni e imprese: "Gli attaccanti fanno squadra, gli attaccanti si fanno la guerra tra di loro. Ma cosi' siamo destinati a perdere". (AGI)

Cybersecurity: Itasec18, serve piano nazionale universita'

(AGI) - Roma, 6 feb. - "Serve un piano straordinario per le universita': oggi non ci sono risorse sufficienti per formare esperti di cybersecurity". Lo ha affermato il presidente del Cini Paolo Prinetto, intervenuto nel corso di Itasec18 per presentare il libro bianco "Il futuro della cybersecurity in Italia: Ambiti Progettuali Strategici". Il documento sottolinea infatti una forte domanda da parte del mercato, spesso non soddisfatta. "Nei prossimi anni - conferma Paola Inverardi, Rettrice dell'Universita' dell'Aquila - il mondo del lavoro chiedera' centinaia di migliaia di persone in settori specifici che noi non siamo in grado di formare". Inverardi sottolinea, in fatto di cybersecurity, la necessita' di "una formazione ordinaria, rivolta a tutti e su tutto il territorio nazionale". (AGI)

Cybersecurity: Pansa (Dis), Stato regoli operatori come Google

(AGI) - Roma, 6 feb. - "Servono regole per gestire le informazioni" e gli operatori che utilizzano i nostri dati, come Google e Facebook. E' in gioco "l'ordinamento democratico". Lo ha affermato Alessandro Pansa, direttore generale del dipartimento delle informazioni per la sicurezza (Dis), intervenuto nel corso di Itasec18, evento sulla cybersecurity organizzato dal Cini. "La sicurezza informatica comprende tutto e richiede una cultura generalizzata, non solo tecnologica" perche', continua Pansa, "non c'e' piano di sviluppo senza sicurezza". (AGI)

Cybersecurity: falla del Comune Milano rilevata da "hacker buoni"

(AGI) - Roma, 7 feb. - "Gli white hat, gli hacker buoni, sono fondamentali". Lo ha affermato Roberta Cocco, assessore alla trasformazione digitale e servizi civici del Comune di Milano, intervenuta nel corso di Itasec18, la conferenza sulla sicurezza informatica organizzata dal Cini. "La scorsa settimana - ha raccontato Cocco - il network degli hacker del team digitale guidato da Diego Piacentini ci ha segnalato una vulnerabilita' molto seria, che in 24 ore e' stata vista e coperta". Senza il supporto dei "cappelli bianchi - ha ammesso Cocco - non ce ne saremmo mai accorti internamente perche' non abbiamo le risorse e le competenze per farlo". Nel corso di Expo, ha affermato l'assessore, i tentativi di violazione sono stati "qualche migliaio". (AGI)

M5S: Zanero (Polimi), segnale devastante per l'hacking etico

(AGI) - Roma, 7 feb. - "Un segnale devastante per il mondo dell'hacking". Cosi' Stefano Zanero, professore del Politecnico di Milano e tra i massimi esperti italiani di cybersecurity, definisce all'AGI la denuncia di Evariste Galois, il "white hat" (cappello bianco, cioe' hacker buono) denunciato dal Movimento 5 Stelle per aver violato la piattaforma Rousseau. "Si confonde - afferma Zanero - un hacking etico che (magari senza rispettare tutte le norme) cerca una vulnerabilita' per portare un contributo positivo, con chi commette azioni che hanno la violazione come unico

obiettivo". Zanero, che in questi giorni e' general chair di Itasec18, evento organizzato dal Cini e dal Laboratorio nazionale di Cybersecurity, definisce la vicenda "un passo indietro" anche sul piano della comunicazione, perche' "mescola due figure che hanno fatto due cose ben diverse". Da una parte Evariste Galois, indagato per aver segnalato una vulnerabilita'; dall'altra R0gue0, un hacker "nero" (non ancora identificato) che, dopo essersi intrufolato in Rousseau, ha rivelato documenti e dati sensibili. Zanero definisce "ridicola" la denuncia e conferma quanto scritto su Twitter: "Mi offro pro bono come consulente tecnico di parte" per sostenere Luigi Gubello (il nome offline di Evariste Galois). "E come me ci sono tanti altri colleghi pronti a farlo". (AGI) Di2/Gav (Segue)

M5S: Zanero (Polimi), segnale devastante per l'hacking etico (2)

(AGI) - Roma, 7 feb. - "Spero che a livello giudiziario si risolvera' in una bolla di sapone - continua - ma il danno e' gia' fatto. Di Maio ha dichiarato di aver identificato l'hacker e ha accusato un ragazzo di avere dei mandanti". Alla base c'e' "un problema culturale: dovremmo trasmettere l'idea che chi scopre vulnerabilita' e le segnala, anche usando metodi non ortodossi, non e' un criminale. E' un dibattito che va avanti da troppo tempo. Servirebbe un chiarimento a livello normativo" che definisca una volta per tutte cosa sia l'hacking etico. Il timore riguarda, a questo punto, le possibili conseguenze. Non solo per Evariste Galois: "Vedere che anche con le migliori intenzioni si puo' finire nei guai e' un disincentivo" per altri "cappelli bianchi". La vicenda Galois-M5S sarebbe, secondo Zanero, indice di quanto sia lontana l'ipotesi che aziende, partiti e pubblica amministrazione italiani si aprano ai "bug bounty program", cioe' a quei programmi che ricompensano gli hacker se individuino falle senza sfruttarle. "Non credo ci siano le condizioni, ne' nel mondo privato ne' nel pubblico. Perche' l'incentivo economico segue un riconoscimento dell'hacking etico, che ancora non c'e'. In un bug bounty program ti dovrebbero pagare. Qui sarebbe gia' un passo avanti essere ringraziati invece che denunciati". (AGI)

Cybersecurity: Cisco, tecnologia sola non basta,serve collaborare

(AGI) - Roma, 8 feb. - "La cybersecurity e' al centro dello scenario tecnologico e da essa dipende la nostra capacita' di assicurare alle persone, alle imprese, al paese la possibilita' di cogliere le opportunita' della trasformazione digitale. Per questo la cybersecurity e' uno dei focus piu' importanti del nostro piano di investimento Digitaliani, con cui dal gennaio 2016 ci stiamo impegnando per accelerare la digitalizzazione dell'Italia". Cosi' l'ad di Cisco Italia, Agostino Santoni, intervenendo a ItaSec, conferenza nazionale sulla sicurezza informatica organizzata dal Laboratorio nazionale di cybersecurity del Cini a Milano. "La vera sfida e' quella di migliorare innanzitutto la comprensione del panorama attuale delle minacce e delle prassi di sicurezza, e poi di adeguare strumenti e modalita' di intervento ai nuovi modelli operativi e ai rischi cyber emergenti", ha spiegato il manager, "prima di tutto e' necessario avere un fondamento tecnologico forte e usare la rete come componente chiave su cui basare tutta la cybersecurity". Negli ultimi anni, ha spiegato ancora Santoni, "Cisco ha investito miliardi di dollari in acquisizioni strategiche nell'ambito della sicurezza informatica e in innovazione interna per essere sempre un passo avanti e pronta a far fronte alla maggior parte di attacchi. Inoltre, avendo installato e gestendo l'80% delle reti a livello globale, Cisco ha una visibilita' sulla rete senza precedenti, e una strategia che fa della rete

l'elemento fondamentale di enforcement della sicurezza. Una rete in grado di imparare e di adattarsi istantaneamente alle minacce e di proteggersi da sola". Se la tecnologia e' alla base della protezione, da sola non e' sufficiente: deve essere affiancata da nuove forme di dialogo e di cooperazione, anche strutturata, con i clienti e i partner, ma anche con gli altri attori del settore e con le istituzioni. Per Santoni, "un esempio concreto e' rappresentato dal progetto che stiamo portando avanti con il Comune di Milano, l'iniziativa Safer Milan, progetto di sperimentazione a 360 gradi per rendere la citta' ancora piu' smart e sicura, con un Security Operation Center, un centro di competenze per l'innovazione e iniziative di formazione per i giovani nel settore della cybersecurity". Quindi Santoni ha puntato l'attenzione sull'elemento fondamentale della diffusione di competenze digitali qualificate per questo settore: "All'interno del nostro piano - ha concluso - l'offerta formativa del programma Cisco Networking Academy si e' arricchita di corsi specifici sulla cybersecurity e altre tecnologie che mirano a raggiungere 100.000 studenti nell'arco di tre anni. Con queste azioni mirate stiamo mettendo a disposizione dei migliori talenti la nostra esperienza nel settore per fare emergere le soluzioni che permettono di sventare le minacce di oggi e di domani". (AGI)

Itasec18: Pinotti a Milano per sicurezza informatica

(AGI) - Milano, 8 feb. - Il ministro della Difesa Roberta Pinotti interverra' questo pomeriggio a Itasec18, la conferenza nazionale sulla sicurezza informatica organizzata dal Laboratorio Nazionale di Cybersecurity del Cini, in corso da ieri e fino al 9 febbraio al Politecnico di Milano. Pinotti partecipera' al convegno in programma alle 15,30. I lavori vanno avanti tutto il giorno con esperti, ricercatori e professionisti dal mondo accademico, industriale e governativo nel campo della sicurezza informatica e importanti speaker istituzionali. (AGI)

Macerata: Pinotti, sicurezza non diventi un ring

(AGI) - Milano, 8 feb. - "Rafforziamo la democrazia e chi si occupa di sicurezza ma evitiamo che il tema della sicurezza diventi un ring su cui si misurano parole, che possono diventare poi azioni terribili e illegali". E' l'auspicio del ministro della Difesa Roberta Pinotti, che a margine di Itasec18, un evento sulla cybersecurity, ha commentato il crescente clima di odio dopo i fatti di Macerata e le minacce al ministro Orlando dopo la visita ai feriti nel raid razzista. "Siamo rimasti tutti impressionati e colpiti non solo dagli avvenimenti ma anche dal fatto che sui social, su un avvenimento terribile come un tentativo di strage di persone inermi - aggiunge - si sia trovato chi ha sostenuto un'azione di questo tipo". "Chi ha responsabilita' politica - dice con fermezza - deve dire che l'odio e' quanto di piu' terribile si possa proporre e ispirare. Le parole sono pietre quindi chi ha responsabilita' politica deve pesarle molto bene". Quanto alla decisione del prefetto, che su invito del sindaco, ha vietato tutte le manifestazioni a Macerata, inclusa quella antirazziste in programma per sabato, il ministro Pinotti commenta dicendo che "oggi quello che c'e' da fare e' raffreddare il clima". "Io ho visto che anche il sindaco di Macerata e' preoccupato per un aumento della tensione - aggiunge - e ha ritenuto questo opportuno. Lo hanno valutato loro che conoscono la citta'". (AGI)

== Fake news:Pinotti, tossine eversive per debilitare democrazia

(AGI) - Milano, 8 feb. - "Le 'false notizie' non sono, banalmente, la diffamazione o la calunnia. Sono tossine inoculate con estrema perizia negli organismi sociali, non per uccidere ma, in genere, per debilitare, facilitando poi l'attuazione di disegni che possono avere anche carattere eversivo di un ordine sociale e politico". Lo ha detto il ministro della Difesa Roberta Pinotti intervenendo a Itasec18, la conferenza nazionale sulla sicurezza informatica organizzata dal Laboratorio Nazionale di Cybersecurity del Cini, al Politecnico di Milano. "Non e' colpa di internet, o dei social media, se questo avviene; lo sappiamo tutti - aggiunge Pinotti - . Pero' sappiamo che questa minaccia e' cosi' seria, potenzialmente devastante, proprio perche' la rivoluzione tecnologica degli ultimi quindici anni ha trasformato, profondamente, la struttura dei rapporti sociali, rendendo obsoleti anche gli strumenti tradizionali posti a tutela della democrazia e delle libere istituzioni". Il ministro ha ricordato che all'inizio del suo mandato volle preparare un Libro Bianco sulla sicurezza internazionale e la difesa, dopo piu' di dieci anni dal precedente, e quindi conosce bene le difficolta', ma anche il valore che e' contenuto in una elaborazione di questo tipo. "La conoscenza dei rischi per il sistema economico, per l'industria, per i servizi, determinati da azioni ostili e criminali sulla rete, e' ormai, finalmente, patrimonio condiviso - ha osservato Pinotti - . Non e' diffusa la competenza, in termini di sicurezza cibernetica, ma quantomeno e' diffusa la consapevolezza della minaccia, e questo e' gia' un primo importante passo in avanti che abbiamo saputo compiere in questi ultimissimi anni". (AGI)

Sicurezza: Pinotti, consapevolezza rischi cyber no sufficientemente ampia

(AGI) - Milano, 8 feb. - Sulla sicurezza internazionale "la consapevolezza dei rischi rappresentati dalle operazioni ostili in campo cyber non e' sufficientemente ampia, al di fuori di un circolo di specialisti ancora troppo ristretto". Lo ha sottolineato il ministro della Difesa Roberta Pinotti intervenendo a Itasec18, la conferenza nazionale sulla sicurezza informatica organizzata dal Laboratorio Nazionale di Cybersecurity del Cini, al Politecnico di Milano. "Tutto cio' vuol dire che un attacco cibernetico di ampia portata puo' essere considerato opera di hacker particolarmente agguerriti, magari che operano con fini criminali o anche ideologici - aggiunge - oppure puo' essere considerato la fase iniziale di una guerra vera, destinata di li' a poco a tramutarsi in uno scontro militare tradizionale. E non e' difficile immaginare, a questo punto, quanto possa essere pericolosa per la pace e la sicurezza internazionale l'azione ostile condotta nel cyber-spazio". Pinotti ha poi spiegato cosa sta facendo lo Stato in questo nuovo scenario per contrastare e prevenire le minacce. E insieme alla necessita' per lo Stato di agire come "rete delle reti", cioe' come "federatore di capacita' e competenze diverse e diffuse, da mettere a sistema per assicurare resilienza e risposta", molto importante e' l'entrata in azione del Comando Interforze per le Operazioni Cibernetiche, il CIOC. "L'impulso per la sua costituzione viene proprio dal Libro Bianco per la difesa - spiega - In due anni siamo passati dal nucleo iniziale del Comando a questo primo traguardo di "capacita' iniziale". Per un altro anno almeno continueremo a far crescere le capacita' di questo Comando, per portarlo a pieno regime". I compiti sono in generale quelli connessi con tutte le varie tipologie di operazioni che si svolgono nell'ambiente cibernetico. (AGI)

Cybersecurity: Soro, protezione dati sia priorita' per politica

(AGI) - Roma, 9 feb. - "In un mondo connesso e' indispensabile fare della protezione di dati e infrastrutture l'obiettivo prioritario delle politiche pubbliche". Mentre "il dibattito pubblico e' spesso silente su questi temi". Lo ha affermato Antonello Soro, presidente dell'Autorita' Garante per la Protezione dei Dati Personali, intervenuto nel corso di Itasec18, evento organizzato dal Laboratorio nazionale di cybersecurity del Cini. "Oggi - ha sottolineato Soro - c'e' l'idea che l'agenda digitale sia un problema di quantita' e invece dovrebbe essere una questione di qualita'". Soro ha sottolineato ad esempio che "in Italia i gestori raccolgono miliardi di tabulati telefonici e dati e li conservano a lungo, molto lungo, in banche dati vulnerabili". Le imprese non hanno ancora compreso che "la protezione dei dati non e' un costo ma una risorsa. Se un'imprese non protegge il proprio patrimonio digitale, lo perde e lo consegna ai propri avversari". (AGI)

Cybersecurity: Soro, hacker 'bianchi' andrebbero incoraggiati

(AGI) - Roma, 9 feb. - Gli hacker 'bianchi', cioe' chi individua le vulnerabilita' informatiche e le segnala senza sfruttarle, "andrebbero incoraggiati e remunerati". Lo ha affermato Antonello Soro, presidente dell'Autorita' Garante per la Protezione dei Dati Personali. "Abbiamo bisogno di convogliare le migliori intelligenze in modo da aiutare la protezione di dati, sistemi e infrastrutture". Soro, intervenuto nel corso di Itasec18, evento organizzato dal Laboratorio nazionale di cybersecurity del Cini, ha fatto riferimento alle recenti brecce aperte su diversi siti che fanno capo a partiti e movimenti politici: "Sono molto vulnerabili. Chi li gestisce non ha reputato abbastanza alto il rischio di vulnerabilita'". Le organizzazioni politiche, invece, "hanno il dovere" di garantire le proprie strutture digitali e "investire in cyberesecurity", non solo "perche' trattano dati sensibili ma anche perche' promuovono il modello della democrazia elettronica. Un modello che potra' essere preso in considerazione solo se sara' sicuro almeno quanto il sistema democratico tradizionale". (AGI)

Cybersecurity: Baldoni (Dis), perseguire chi mette a rischio dati

(AGI) - Roma, 9 feb. - "Dobbiamo stimolare un dibattito per distinguere che cosa e' buono e che cosa e' cattivo nel cyberspazio. E dobbiamo perseguire chi commette reati ma anche chi, con i sistemi obsoleti, mette a rischio i dati". Roberto Baldoni vicedirettore generale con delega alla cyber del Sistema informazioni per la sicurezza (Dis), ha toccato cosi' il tema degli 'hacker bianchi', cioe' coloro che segnalano le vulnerabilita' senza trarne vantaggio, nel corso del suo intervento a Itasec18, organizzato dal Laboratorio nazionale di cybersecurity del Cini. "Non sono affatto sicuro che tutti gli attori istituzionali abbiano compreso che la cybersecurity e' una priorita' e ha bisogno di investimenti. Nessuno - ha aggiunto - e' fuori dallo spazio digitale: infrastrutture, sanita', ministero dell'Istruzione. Ma anche i privati devono capire che un sistema resiliente non puo' essere a carico del governo. Ognuno deve fare la propria parte". "Serve creare - ha concluso il vicedirettore del Dis - un ecosistema della cybersicurezza, fatto da ricerca, industria, governo".