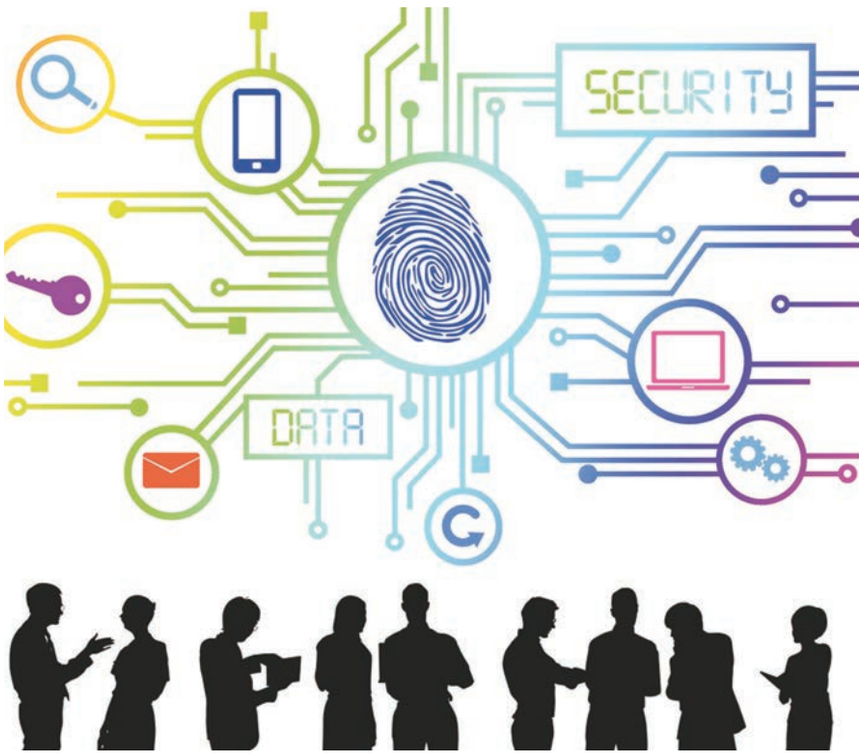
# Un Ppp in cybersecurity

L'esponenziale crescita delle cyber minacce da un lato, e il continuo adeguamento delle normative di protezione dei dati impongono un serio ripensamento, organico, del settore. Il 25 maggio all'Usi un evento cercherà di 'fare il punto'.

**Alessandro Trivilini, Responsabile del Servizio informatica forense della Supsi e rappresentante per la Svizzera nel programma intergovernativo di cooperazione europea Cost per la ricerca scientifica e tecnologica.**




La resilienza degli attacchi informatici e la loro imprevedibilità, in rapporto ai rischi cyber, impongono un cambio di mentalità nella gestione in azienda della cybersecurity. Poco male, una necessità che apre la strada a molte opportunità di crescita, sviluppo e business. Gli addetti ai lavori concordano che è tempo di definire nuove modalità di organizzazione delle politiche di sicurezza, sempre più di carattere interdisciplinare. Mai come ora è necessario fare squadra, aggregando esperienze, competenze e soprattutto talenti, per arginare una modalità operativa ormai obsoleta che vede nella figura del classico amministratore di rete una congestione di responsabilità non più sostenibile.

Da qui, l'esigenza di offrire alle aziende del Canton Ticino l'occasione di incontrare e conoscere giovani talenti preparati alle nuove sfide, con un imprinting di carattere interdisciplinare, maggiormente orientato alla gestione di tutto il processo cyber. Un processo complesso che prevede aspetti di prevenzione, preparazione e reazione. Nelle prime due categorie troviamo competenze sulla governance, l'audit e l'education, mentre la terza prevede, tra le altre cose, l'incident response, la digital forensics e la blockchain analysis.

Tra i contesti di applicazione maggiormente toccati da queste competenze, nella nuova società digitale in fase di sviluppo, emergono con forza il FinTech, l'Internet of Things e il Cloud Computing.

In questa prospettiva strumenti software e apparecchiature hardware sono estremamente necessari ai fini di un'adeguata protezione, ma per essere efficaci devono poter essere scelti, aggiornati e integrati nel business aziendale con oculata e ponderata lungimiranza. Questa attitudine contempla una complessità decisionale non sempre facile da capire, per chi in azienda deve percepire le strategie di cybersecurity come un investimento (ormai imprescindibile) e non più come un costo da inserire a preventivo nella colonna "varie ed eventuali". Un cambio di marcia, come dicevo, che trova molta forza propulsiva nelle collaborazioni strategiche in perfetto stile public-private-partnership.

Con l'applicazione del Gdpr europeo e la revisione totale della legge svizzera sulla protezione dei dati (Ldp), il dato digitale assume un valore senza precedenti. Diventa il protagonista indiscusso di scenari ancora tutti da scrivere, sia per le opportunità che per le conseguenze in caso di scarsa gestione e pianificazione. Cambia quindi il suo valore e con esso cambia l'attitudine di chi è chiamato a gestirne la sicurezza. È evidente che non può più essere considerata soltanto come una serie di interventi puntuali finalizzati all'aggiornamento dell'antivirus e dei sistemi operativi,

ma come un processo continuo e interdisciplinare in costante evoluzione.

Ecco perché se in azienda, come nelle Istituzioni, non cambia la mentalità verso la difesa cyber, il rischio è che le risorse informatiche non bastino mai. Ad ogni nuovo attacco qualcuno potrebbe reclamare una nuova risorsa interna specializzata per comprendere, affrontare e mitigare le molteplici sfumature caratterizzanti l'attacco subito. E in quest'ottica, purtroppo, la gestione della cybersecurity potrebbe sfociare in una 'neverending-story' mangia soldi.

Anche perché lo abbiamo capito tutti, i crismi di sicurezza necessari per la gestione della complessità delle infrastrutture critiche e della volatilità del dato digitale, devono costantemente fare i conti con un nemico invisibile e in parte imprevedibile chiamato fattore umano. Ma allora cosa fare per porsi in una posizione di vantaggio rispetto a chi ha scelto come modello di business l'attacco informatico?

Una delle possibili risposte trova fondamento nelle caratteristiche che rendono il Cantone Ticino, per la sua posizione geografica strategica, attrattivo e interessante per nuove sinergie tra pubblico e privato. Di fatto, la filiera dell'innovazione scientifica in ambito cyber non può più prescindere dal coinvolgimento diretto di ricercatori preparati scientificamente allo stato dell'arte per dare supporto alle aziende che hanno l'arduo compito di trasformare idee, visioni e progetti in prodotti e servizi ad alto valore aggiunto, capaci di innovare e generare benessere comune.

Siamo un piccolo ma importante hub al centro dell'Europa, per questo non possiamo trascurare ciò che ci circonda. In particolare, le strategie cyber della comunità europea e gli investimenti che ha deciso di fare (oltre 450 milioni di euro) per lo sviluppo di collaborazioni in stile private-public-partnership, per il periodo 2017-2020, attraverso il programma di ricerca e innovazione Horizon 2020.

Un segnale chiaro e concreto che indica la strada da seguire per meglio cogliere le numerose opportunità di sviluppo attorno al nostro Paese. La cybersecurity è diventata ormai un fenomeno globale e globalizzante, in cui la territorialità del dato digitale e della difesa cyber non possono più essere circoscritti ai soli confini locali tradizionali.

A questo proposito, l'Associazione Ated Ict, attiva in Ticino da quasi mezzo secolo, pone le basi per lo sviluppo nel Cantone Ticino di nuove e importanti sinergie, utili a sfruttare le molteplici opportunità che il campo della cybersecurity offre.

Ciò attraverso l'organizzazione di eventi tematici interdisciplinari e il coinvolgimento diretto di Istituzioni e aziende locali, nazionali e internazionali. A gennaio del 2017 è stata ufficialmente creata una sezione dedicata proprio a questo scopo, grazie anche al coinvolgimento diretto dell'Associazione svizzera per la sicurezza delle informazioni (Clusis) e del Servizio di informatica forense Supsi. Una triade aperta e accessibile ad altri stakeholder, che attraverso l'organizzazione di molteplici occasioni di scambio ha permesso di ospitare in Ticino diversi professionisti di fama internazionale attivi nel campo della cybersecurity, con i quali è stato possibile condividere conoscenze, esperienze e contatti utili per lo sviluppo in Ticino di nuove opportunità di business.

Ated Ict crede fermamente che poter disporre sul territorio di un network d'eccellenza sia di buon auspicio per tutte le aziende e le Istituzioni interessate ad affrontare la cybersecurity in stile public-private-partnership.

## 25 maggio, il Gdpr all'Usi

È in tale data, del resto, che verrà dato il via ufficiale alla nuova disciplina europea in tema di trattamento dei dati. Presso l'aula magna dell'Università della Svizzera Italiana avrà luogo un importante evento di approfondimento, organizzato dall'Ated e destinato a imprenditori e addetti ai lavori, oltre che ricercatori, direttamente coinvolti quotidianamente proprio in tale tematica. Per quanto infatti manchi ormai poco al varo delle nuove normative, la confusione è notevole, e solo in pochi hanno già individuato le misure concrete da adottare per allinearsi al regolamento europeo. Tali informazioni sono e saranno centrali per il core business di centinaia di imprese, pubbliche e private, oltre che per le stesse pubbliche amministrazioni, e gli enti di ricerca, nell'immediato futuro. Quattro le aree fondamentali del nuovo Regolamento generale sulla protezione dei dati (Gdpr) indagate: ricerca e innovazione; aziende e industrie; Pa e istituzioni; sicurezza e cyber difesa. L'evento, dalle 9.00 alle 14.00, verrà moderato da Alessandro Trivilini, responsabile del servizio di informatica forense della Supsi, interverranno in qualità di relatori: Norman Gobbi, consigliere di stato del Canton Ticino; Antonio Carzaniga, decano della Facoltà di scienze informatiche dell'Usi; Zoltan Szekely, avvocato e membro dell'Europol Data Protection Experts Network (Eden); Paolo Lezzi, Ceo di InTheCyber; Zulay Managanaro Menotti, avvocato dell'Unione Europea dal Consejo General de la abogacia Española, e Rocco Taller, avvocato dello studio legale Talleri Law.

Per ulteriori informazioni: https://www.ated.ch/il_giorno_del_big_bang.jsp

**Sopra, il campus di Lugano della Università della Svizzera Italiana, dove si terrà l'evento.**